Risk based internal auditing

Compiling a Risk and Audit Universe

David Griffiths

PhD FCA

www.internalaudit.biz

Version 2.0

Contents

Contents

Contents 1
Introduction 1
1 The basics 2
1.1 What are we trying to do? 2
1.2 Where do we start? 2
1.3 Summary 3
2 Finding the objectives and risks 5
2.1 Adequacy of any existing ORCR 5
2.2 Identifying objectives 5
2.3 The sources of opportunities and risks 5
2.4 Identifying opportunities and risks 6
2.4.1 Ways of identifying opportunities and risks 6
2.4.2 Interviewing 6
2.4.3 Risk workshops 6
2.4.4 The accounts 6
2.4.5 Legislation and standards 7
2.4.6 COSO 7
2.4.7 Audit files 8
2.4.8 Processes and Systems 9
2.5 Decision making processes 9
2.5.1 Decisions making - the basics 9
2.5.2 Decision making - the detail 9
2.5.3 Provide support for decision making 11
2.5.4 The internal auditing of decision making 12
2.6 Summary 13
3 Organizing the objectives and risks 14
3.1 Introduction 14
3.2 First level objectives 14
3.3 First level opportunities and risks 14
3.4 Second level objectives and risks 15
3.5 Subsequent level objectives and risks 15
3.6 Strategies 16
3.7 Accounting systems 16
3.8 The ORCR 19
3.9 Lessons learnt 19

4 Managing opportunities and risks 20
4.1 Introduction 20
4.2 Risk scores 20
4.3 Opportunity scores 21
4.4 Risk Appetite 21
4.5 Risk ownership 21
4.6 Internal controls 21
5 Planning 22
5.1 Risk and Audit Universe 22
5.2 Deciding on audits 22
5.3 Processes 23
5.4 Functions 23
5.5 Next steps 23
6 Appendices 24
6.1 Appendix A - Interviewing 25
6.2 Appendix B - Running a risk workshop 26
6.3 Appendix C - Level 1 objectives and risks mind map 29
6.4 Appendix D - Expanded mind map example 30
6.5 Appendix E - Typical accounting system controls 31
6.6 Appendix F - Audit tests for the decision-making process. 35
7 Version control 38

Introduction

I've been involved with the compilation of two Risk and Audit Universes from Objectives, Risks and Controls Registers (ORCR) but the first wasn't very comprehensive. The second was restricted in scope, as it was a small housing charity, and this ORCR can be downloaded at www.internalaudit.biz. The books I have written and made available on this site are intended to provide ideas as to how to set up a comprehensive ORCR and use it to generate a Risk and Audit Universe.

This book is part of a series:

1. *Book 1: Risk based internal auditing - an introduction*. This introduces risk-based principles and details the implementation of risk based auditing for a small charity providing famine relief, as an example. It includes example working papers.
2. *Book 2: Compilation of a risk and audit universe*. (This book). Book 2 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 a risk based internal audit of accounts payable. It is based around the actual working papers, similar to those in the audit from Book 1.

Since I'm retired, for the purposes of this book I had to make up a company, I'm assuming the organization compiling the RAU to be a retail business with around 100 stores. It is a company with shareholders, listed on the local stock exchange. It has not purchased software to record risks and controls.

So this book is intended to provide a few ideas about compiling a risk and audit universe (RAU) and then using it. It is not intended to be a definitive guide, or to represent 'best practice'. It does assume knowledge of risk based internal auditing gained by reading ' Book 1 - 'Risk based internal auditing - an introduction' available from www.internalaudit.biz and is intended to provide more detail than is in that book.

The RAU must not be seen as an 'end'. The work of an internal audit department doesn't stop when the RAU is compiled, that's when it starts! The RAU provides the foundations for planning, delivering, monitoring and reporting of the work of the department.

I have used the term 'board' in the book for the ultimate authority of an organization, which is also known as the 'C-suite'. In organizations with an Audit Committee, this may take the place of the board in some circumstances, such as the receipt of internal audit's opinions.

The IIA have now produced a Practice Guide 'Developing a Risk-based Internal Audit Plan'. About five years after the first version of this book but you probably should read it.

1 The basics

1.1 What are we trying to do?

In Book1 1 'Risk based internal auditing - an introduction', I defined internal auditing as:

> **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 internal audit function within an organization is therefore aiming to help that organization achieve its objectives.

Thus the internal audit department needs to know:

- What are the objectives throughout the organization?
- What opportunities have been recognized to benefit these objectives?
- What risks threaten these objectives?
- What controls should be in place to manage these opportunities and risks?
- What tests have been carried out, or should be carried out, to check the proper operation of these controls?
- What is the result of these tests?

Knowing these results, the function can then present an opinion to the board about the likelihood that objectives will be achieved. This is what most boards want from their internal audit function.

Thus our initial aims are to document:

- The objectives set by the organization.
- The opportunities benefiting the achievement of these objectives.
- The risks threatening the achievement of these objectives
- The internal controls managing these risks
- The audit checks we need to carry out to ensure these internal controls are operating properly

I'll refer to this document as a risk and audit universe (RAU), although it starts with objectives, through risks and controls to the audits checking them.

When we have carried out the audit checks we will then be able to deliver an opinion to the board.

1.2 Where do we start?

The organization should have compiled a risk register. This should show the objectives of the organization, the opportunities/ risks whichy benefitting/threaten their achievement and controls managing them. I refer to this as the organization's Objectives, Risks and Controls Register (ORCR). Assuming this has been approved by the board, it is these objectives on which the board will require an opinion as to whether they are being achieved, and are likely to be achieved into the future.

It is possible that the ORCR will not be sufficiently detailed for use as the risk and audit universe; however it must form the basis. There can be no separate internal audit ORCR, since this is effectively saying to the board that the risks it has identified are inconsequential and internal audit knows best.

However, the state of the ORCR will be dependent on the risk maturity of the organization - see Book 1 and associated IIA publications. An ORCR may not exist, or may be so deficient, in the opinion of internal audit, as to be useless even as a record of the organization's significant risks. In this case the board must be made aware of this by internal audit and the situation remedied by the board. Unilateral action by internal audit in setting up a separate register is not an option.

The ORCR should have been compiled by specifying the objectives of the functions concerned and then managers identifying the risks threatening those objectives, although internal audit may have facilitated this process. This presents a potential problem in that it effectively means that management are defining internal audit's plan, thus jeopardizing the independence and objectivity of internal audit. This overlooks one important principle; it is internal audit's first priority to ensure that the ORCR is complete and accurate, for example in relation to the scoring of risks, and is therefore suitable as a basis for the RAU.

The ORCR will need constant maintenance and should therefore have one function responsible for gathering updates on opportunities and risks and updating the register (the ORCR 'guardians'). This function may be internal audit, or may be a 'risk management' function. If it is a function external to internal audit, a close relationship must be maintained between the two as changes to the register will affect the audits to be carried out and internal audits will discover risks not in the register. There is ample opportunity for disagreement here but a failure to maintain the register as a complete and accurate record of risks is a major internal control deficiency. Disagreement will be lessened if the principles and responsibilities for the custody and maintenance of the register are documented.

There is disagreement among risk managers and auditors about the value of 'risk registers'. They are considered by some to be a bureaucratic exercise which does not contribute to the most important process in an organization: decision-making. However, even if risk registers aren't necessary to fulfill any disclosure requirements of risks, the Chief Audit Executive (CAE) has to have a complete understanding of all risks in order to be able to recommend to the Audit Committee those whose controls should be checked. This risk register (i.e. the OCRC) must add value to the organization.

- The opportunities and risks must be derived from objectives.
- The OCRC must contain both opportunities and risks arising from processes and decisions.
- The appearance of new opportunities and risks must be constantly monitored and the register updated
- The audit plan based on the OCRC must change as a result of changes to objectives, opportunities or risks.

1.3 Summary

- The risk and audit universe is a list of the objectives within an organization, their opportunities and risks, controls and audit checks which enables Internal Audit to deliver an opinion.
- The starting point for the RAU must be the organization's ORCR.

- If the ORCR does not exist, or is so deficient as to be useless even as a record of the organization's significant opportunities and risks, the board must be made aware of this by internal audit and the situation remedied by the board.
- A close relationship must be maintained between the guardians of the ORCR and internal audit, as changes to the register will affect the audits to be carried out and internal audits will discover risks not in the register.
- The principles and responsibilities for the custody and maintenance of the register must be documented.

2 Finding the objectives and risks

2.1 Adequacy of any existing ORCR

Book 1 'Introduction to RBIA' gives greater detail about the 'risk maturity' of organizations and the adequacy of the ORCR. Because there are so many possibilities concerning the adequacy of the ORCR, I will assume that there is no ORCR and that the internal audit department has been given the task of compiling one for approval by the board. Once the ORCR has been compiled, audit checks can be added to form the risk and audit universe (RAU).

2.2 Identifying objectives

Before we can identify risks, we have to identify the organization's objectives. Ideally they will be in writing, clearly labeled as aims, objectives or mission statements. They may be found in:

- Published accounts
- Other published documents for shareholders and customers, possibly on the company's website
- Internal documents, possibly on the organization's intranet
- Targets set for employees, publicly or as part of their appraisal.

The objectives should have been defined by the organization's governing body, for example, the board of directors or trustees. These objectives should have been sub-divided for each job holder, so that everyone working for the organization knows their objectives.

If they are not easily available, the governing body should be made aware of this deficiency and asked how they will address it.

2.3 The sources of opportunities and risks

Opportunities and risks (O&R) may arise from several sources:

- The business: O&R come from the type of work the organization carries out. It is from the business that the best opportunities will probably arise.
- Process risks: O&R come from the systems the organization uses to achieve its objectives. A hospital which uses purely manual procedures to record patients' treatment will have different risks to one that records treatment on a computer. There may be opportunities to improve the efficiency of processes.
- External risks; O&R come from a variety of sources; governments (tax changes); the planet (floods); the universe (asteroids). Some of these risks can be managed; some may have to be tolerated. Opportunities may arise, for example from new legislation and tax breaks.
- Decision risks: O&R arise from the decisions made throughout the organization.

The first three risks arise from the work being carried out to achieve the organization's objectives. The controls to manage them are usually part of the organization's processes and can be verified ('ticked') by internal audit.

Because the decisions made vary throughout the organization, the management of these risks may not be easily verifiable. More details are given in Book 1 and later in this book.

2.4 Identifying opportunities and risks

2.4.1 Ways of identifying opportunities and risks

Book 1 'Risk based internal auditing - an introduction' lists three ways of identifying risks:

- Interviewing
- Risk workshops
- The accounts

These are 'internal' sources of risk which should be identified by the management of the company, with the 'risk guardians' prompting where necessary (particularly in the case of IT and accounting risks).

2.4.2 Interviewing

The output from an interview is an individual's view of the opportunities benefitting, and risks hindering, the achievement of 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 opportunities and risks than from a meeting.

The disadvantages are:

- The wide range of opportunities and 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 6.1.

2.4.3 Risk workshops

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

Risk workshops can be used:

- With the most senior people in an organization, to get the significant opportunities and risks.
- With members of a project team, to highlight the opportunities that might arise, and the risks which might threaten, the successful conclusion of the project.
- With people involved in an audit, to highlight any issues already known.

The advantage of a risk workshop, over interviews of individuals, is that people interact with each other to produce new ideas. 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 6.2.

2.4.4 The accounts

We should examine the detailed management 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 opportunities and 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. For example, if bad debts are low does this imply that opportunities are being missed by not selling to customers who are considered even a very low credit risk?

2.4.5 Legislation and standards

There are other ways of identifying objectives and risks, particularly those affecting specialist areas such as taxation, accounts, health and safety. These include:

- Legislation, such as tax and company law; health and safety requirements.
- Requirements set by stock exchanges, banks, local councils and franchising companies.
- Standards set by professional bodies and legislators, such as the IIA, COSO, chartered (public) accountants and chartered surveyors.
- Standards required by organizations, such as rules governing care of vulnerable adults. These are effectively 'internal controls' already identified and addressing risks but they need to be included in the RAU.

These are 'external' sources of risk. Some will be identified by management, particularly specialist risks such as those involving health and safety, product legislation and property law. Some risks may be identified by the 'risk guardians' and internal audit. These should be agreed by the managers responsible for controlling the risks.

Including objectives and risks from the above sources is to include 'Compliance Auditing' in the RAU, but in a form where the objectives and risks which require the controls are clearly identified.

If you are a US reader, I have set up a separate branch based on the COSO Integrated Framework for internal controls (see below). There is also a global standard (ISO 31000 Risk management – Principles and guidelines’. I have used the check list from this standard to derive internal controls for the objective, 'Establish a risk strategy to determine risks' in the accompanying spreadsheet.

For both of these standards, I have had to set up risks which the controls listed in the standards are intended to mitigate.

2.4.6 COSO

The Committee of Sponsoring Organizations of the Treadway Commission (COSO) is a joint initiative of five private sector organizations, including the IIA. It issued a document 'Internal Control–Integrated Framework' in May 2013 which is an update of a document issued in 1992. To support this document it also issued 'Illustrative Tools for Assessing Effectiveness of a System of Internal Control'. The framework is an important document which was issued as a draft in 2012.

Since the implementation an integrated framework of internal control is a requirement of COSO, it needs to be included as an objective of a US organization (or 'entity' to use COSO's term) and therefore has to be included in the RAU. I have used the 2012 draft (because I am too mean to buy the final document) and I have included it in the RAU as follows:

1. In Objective level 1 'Establish strategies for delivering the objectives' and Risk level 1 'Uncontrolled risks threaten the achievement of objectives' , I have set up Objective' level 2 as 'Establish an internal control framework (COSO)'.

2. There are 17 'principles' in the Framework and I have set these up as level 3 objectives. There are no risks identified, so I have made some suggestions.
3. Each of the principles has 'attributes' attached, which link with paragraphs in the framework narrative. I have taken these attributes as controls, although they are inevitably non-specific. The 'Illustrative Tools' document has forms ('Principle evaluation templates') for inserting the controls in action in order to assess whether there are deficiencies in achieving the attribute.
4. I have then suggested tests which might be used to check that the attribute 'control' is operating, after reference to the appropriate paragraphs in the narrative.
5. Tests fall into one or more of the following categories:
    - 'One-off tests' done as part of a specific audit to look at the correct operation of a principle. For example, a test to ensure that the board have carried out a risk assessment for the top level of the entity; published a code of conduct; or objectives have been established throughout the organization.
    - Tests done as part of an audit which include some specific COSO attributes. For an example, an audit of HR to look at instructions about including the performance of internal controls as a personal target
    - Tests done as part of every audit, which provide evidence about compliance with a COSO attribute. For example, ensuring that management have carried out a risk assessment on their objectives and have identified the controls necessary. As part of the audit opinion, compliance with particular COSO principles can be confirmed, or not, depending on the audit findings.

The first two types of test can be identified as part of a specific audit. The last type of test will appear in most audit programs as a 'COSO' test. Internal control deficiencies will be recorded on the '4 Summary of deficiencies template'. Each audit will provide information to complete '3 Principle Evaluation Templates' for some attributes, which can be used to update '2 Component evaluation templates'. By the end of the year the '2 Component evaluation templates' must be sufficiently detailed to complete the '1 Overall assessment of internal control template'.

The compilation of an ORCR is an essential part of Principle 7 ('Identifies and analyzes risk').

2.4.7 Audit files

Large organizations may have many thousands of risks, which seems rather daunting. However, internal auditors have already identified and recorded these risks and controls in their audit files! They are not recorded in one place, and are not necessarily the right format but they have been identified. So the prospect of gathering risks and controls together shouldn't be too much of a problem and the audit files could be used to establish the bare bones of the ORCR. Since these risks have been identified by internal audit, they should then be agreed by the managers responsible for controlling the risks, otherwise the register becomes the 'property' of internal audit.

The advantage of the RAU is that the relationship between objectives, risks/opportunities, controls and audit tests is clearly seen, which is not the case with audit files.

2.4.8 Processes and Systems

The term 'Processes' can have many definitions. We will take it to mean all the tasks and actions which deliver an objective. Thus we will have processes to make decisions; deliver a set of management accounts; purchase goods for resale; acquire a new store. 'Systems' are normally considered to be the IT programs which are included in processes. These will include, accounts payable, general ledger, stock control and fixed assets.

Risks arising from processes may be buried deep within all the tasks and activities which make up the process, for example a risk that false supplier accounts are set up. They are most likely to be identified as part of the audit work and it is therefore important the ORCR is updated at the end of the audit and approved by management.

It is probably worth mapping out the organization's processes (see the spreadsheet 'Processes' in the RAU workbook https://www.internalaudit.biz/files/rau/rbiacompilationrau.xlsx) and linking this with the RAU, as it may identify areas not identified as having risks. The identification of risks in this way links the RAU with 'Systems Auditing' but, as with compliance auditing, links the audit tests back to internal controls, risks and objectives. As I wrote in Book 1, RBIA is just pushing out the boundaries of internal auditing.

2.5 Decision making processes

2.5.1 Decisions making - the basics

We have seen in Book 1 and in section 2.3 that controls over the decision making processes are not always easily checked. We therefore need to consider how an audit can check that the decision making processes maximize value for the organization. So we need to understand decisions.

What is a decision? It's a choice between two or more options. These options may be a simple yes/no choice or more complex. A decision is also like a physical force; it can change the speed or direction of an organization - unless it's a decision to do nothing.

Why does a decision have to be made? Because an objective has to be achieved.

When does a decision have to be made? Well, that depends on the decision. It may be one forced on us by circumstances. What's the best way to get food to the famine area? Do I try and put this fire out? Do I pay this invoice? I'll call this type of decision 'reactive' since it is forced on us by circumstances.

We may also need to make a decision out of a desire to move forward for example, open a new factory, get married. I call this type of decision 'proactive' since the decision makers are in more control. In an organization, these decisions are usually formally approved for example by the board. Reactive decisions may have to be made very quickly; proactive decisions usually have more time.

2.5.2 Decision making - the detail

We now need to consider the elements of decision making, since these will help in deciding what we need to audit in an organization.

2.5.2.1 Define objectives for adding value

Since decisions should add value, or at least preserve it, it is essential that the governing body should have defined top level objectives for the organization, that is a strategy. These objectives should have been communicated to all relevant job holders (permanent and temporary employees; contractors; volunteers). If the people who will make decisions don't know where they are going, they are not going to be able to make the best decisions to get there.

2.5.2.2 Acquire information to identify opportunities and threats

It is information which often triggers the need for a decision: our company is given the opportunity to buy a competitor, a famine occurs and our charity needs to decide how to send food; a fire alarm rings in the computer centre. If we want to make the right decisions at the right time we need relevant and accurate information as soon as it is available.

2.5.2.3 Make decisions which add greatest value

In order to make the best decisions, there are several requirements

1. Understand why the decision is required

This understanding should come from the information constantly being received and monitored. It should include forecast information designed to highlight what decisions are necessary

2. Know what the decision has to achieve

Knowing why the decision is required (reports of famine in central Africa), we can now define a purpose for the decision: decide on the best way to deliver food to the famine area

3. Understand when the decision is needed

- The information received will probably define the urgency of the decision.
- A target time/date for the decision should be communicated to all involved.

4. Identify all possible options

- Identify all possible options which might achieve our objective.
- Involve all job holders that can contribute to identifying possible options.
- Acquire complete and accurate information for each option. Remember decisions can't change the past so historical information is only useful where it helps to predict the future.
- Where appropriate, the limits placed on the options available to the job holder are defined. For example, a job holder may decide to place an order up to £10,000. Above this value a more senior job holder is required to approve an order.
- Determine advantages and disadvantages of each option. This includes looking at scenarios which will result from each option; opportunities and risks; financial modeling if appropriate.
- Be prepared. If it is unlikely that you will have the time to carefully examine options (such as an unexpected famine resulting from civil war), so plan for foreseeable conditions, such as considering possible routes and means of delivery.

5. Decide on best value adding option

- Taking account of the advantages and disadvantages of each option, decide on the most value adding.

- For major decisions, have an independent review of the decision.

6. Decide on actions required to implement option

Having decided on an option, it now has to be implemented (unless a decision was made to do nothing).

- One job holder (the Project Manager) is charged with coordinating the actions and delivering them on time and within budget.
- The actions required to implement the decision are documented.
- Responsibilities for actions are allocated to suitable job holders.
- Timings are specified for each action and incorporated into an overall plan.
- Targets based on timings and other important factors are assigned to job holders involved.

7. Communicate decision and actions

- Decisions, timings, targets etc. are communicated to all relevant job holders.

8. Monitor progress of the action plan

- In order to reinforce the need to make good decisions and act on them, incorporate targets into appraisals.
- Set up monitoring systems to track progress.
- Regularly report progress back to all job holders who have targets.
- When all actions to implement a decision are complete, prepare a report on lessons learnt and communicate this to all concerned.
- Feed lessons learnt into training.

2.5.3 Provide support for decision making

2.5.3.1 Job holders understand what they can decide

There needs to be a framework for decision making. Job holders need to know what decisions they have to make but in many cases they need to know the boundaries for decision making. For example a job holder may be expected to approve invoices for payment up to £10,000 but those above this value should be approved by a more senior person. This framework needs to be consistent throughout the organization.

- The governing body will approve in writing the overall policy for decision making, usually expressed in monetary amounts.
- This policy is interpreted by senior management into authority limits for each job.
- Authority levels are communicated to all relevant job holders
- Authority levels are included in job descriptions
- Decisions the job holder is required to make are specified in their job description.

2.5.3.2 Job holders know how to decide

There's no point in asking job holders, at any level, to make decisions without ensuring they have the knowledge to make the best decisions. The training they require will depend on the decisions they have to make. Proactive decisions usually have long time-scales giving the opportunity for in-depth analysis, possibly involving complex finance. Thus the decision makers need to be trained in using financial modeling and how to gather and analyze information.

Reactive decisions can require a very different approach, especially when they are 'split-second'. A police officer, faced by a gunman has no time to consider all possible options together with any rules which limit their actions. They have to process all the available information instantly and instinctively know how to act. This requires training before they are put into this situation, including simulated examples of typical situations.

Whatever their job, all job holders need to know that it is their responsibility to identify decisions which will provide opportunities for their organization.

All decision makers need an understanding of the psychological factors which influence decision making.

The following elements are required:

- Induction training of job holders to cover the decisions they have to make
- Training on decision making for all job holders, including:
  - Decisions they need to make and when.
  - The importance of identifying decisions which provide opportunities
  - How to gather information and use it to make reliable forecasts.
  - How to identify options and evaluate these.
  - When to involve more senior management.
  - Factors which influence their decision making.
  - For some jobs, simulation of real events such as: how to plan transport of food required urgently; how to deal with angry customers; how to extract injured passengers from a car crash; how to negotiate with a hostage taker.
  - For project managers charged with delivering a decision: how to manage and monitor the progress of a project.

2.5.4 The internal auditing of decision making

2.5.4.1 Audit approaches

Now we have considered the elements of decision making, we can decide how to audit the processes. Note that internal audit is not auditing the decisions made, that is whether they are 'correct' but whether processes exist to make the best decisions. (Although there may be circumstances when internal audit is asked to examine decisions).

An internal audit can examine decision making processes in two ways:

- An audit specifically covering processes forming part of decision making. This can be used for major pro-active decisions where there is documentation to verify the processes used, or to examine specific topics such as job descriptions, the appraisal process or training.
- As part of any audit, since decisions will be made in all systems being audited. For example, decisions to increase credit limits of customers, decisions to order materials. The evidence available will depend on the degree of control required. Any audit should also include checks on job descriptions, appraisals and training.

2.5.4.2 Audit tests

- We can now complete the RAU for decision making processes. Because decisions are made throughout the organization, the processes could be included anywhere in the RAU. I've decided to include them under the 'Provide support for all the company' objective and they are in the 'Processes' sheet in the RAU Excel workbook (link from Book 2 in www.internalaudit.biz).
- The audit tests are also shown in Appendix F.

2.6 Summary

- Sources of risks may be 'internal' (management), or 'external' (standards and legislation.
- Management is responsible for identifying their objectives and the risks which threaten them.
- 'Risk guardians' and internal audit may assist in identifying risks, but the management responsible for ensuring their control must approve their inclusion in the register.
- Opportunities and risks may arise from the day-to-day operational processes used by the organization ('process risks') or from decision making processes ('decision risks').

3 Organizing the objectives and risks

3.1 Introduction

At this stage we need to think about how to organize the risks and objectives we find. You will know from Chapter 2 and appendix D of the 'Introduction' book that we can build a hierarchy of objectives/risks/objectives/risks and so on until we reach a level where we can identify controls.

One way of recording the objective/risk hierarchy is to use 'mind mapping'. Google has a mind mapping app known as MindMup, which works in its Chrome browser. I have used VisiMap, which has the advantage that it can export to Microsoft Office files and to web pages.

If you don't want to use 'mind mapping software, you could use the 'outline' function available in some word processors.

3.2 First level objectives

I've discussed above how we might find the objectives of an organization. Since there will be a wide range of possible objectives, I'm assuming some broad generic aims for our organization, so the objectives are:

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

Objectives 1 and 7 are based on experience. Objectives won't be delivered unless there is a plan in place to ensure people are clear on their responsibilities and support functions (accountants, IT, lawyers) are necessary to provide specialist help and the 'back office' processes required.

'Trade responsibly' includes setting up a Corporate Social Responsibilities policy and implementing it. 'State how responsibilities are met' is about acknowledging the above responsibilities publicly, reporting on how they are discharged, and being answerable for consequences.

These objectives are similar to those included in the Institute of Chartered Accountants in England and Wales document, 'What should companies be responsible for?' (See www.internalaudit.biz for link).

We can include these objectives on the mind map, or start a spreadsheet as the basis of the ORCR. The mind map for level 1 is shown in appendix C and the ORCR and complete mindmap is in the accompanying Excel Workbook (https://www.internalaudit.biz/files/rau/rbiacompilationrau.xlsx - opens workbook)

3.3 First level opportunities and risks

First level opportunities and risks should be identified by the board in a risk workshop. In practice they will suggest a wide range of risks to the objectives which must be included in the ORCR but not all will be at the first level.

Some level 1 risks are shown on the appendix C mind map. The opportunity 'Make the best value adding decisions' has been added to objective 7, 'Maintain support functions'. In practice this opportunity is in all levels of the organization and specific opportunities (accept a new credit customer for example) would be in the credit control section of the OCRC.

Before running a risk workshop with the board, it might be useful to run one with internal auditors, interested managers and risk managers. This will provide experience in running workshops and put a few risks in our 'back pocket' to suggest at the workshop, if required.

We can build the opportunities and risks into the mind map and add our own suggestions as necessary, since we will be submitting the ORCR (or a summary of it) back to the board as part of our reporting process.

There is a danger that the absence of a control may be taken as a risk. For example, 'Invoices are not authorized'. However, if a risk occurs it always leads to a hindrance of the objective, which is not necessarily the case if a control is not performed. In the example the risk is, 'Invoices are paid where goods or services have not been received'.

3.4 Second level objectives and risks

We have now identified at least some of the risks to the level 1 objectives and now have to decide on the internal controls to manage them. In practice, the internal controls required to manage the level one risks will probably not be sufficiently specific to treat as a task which can be audited. For example:

Objective level 1: Maintain profit of existing business.

Risk level 1: Products fail to meet legal and health requirements.

Internal control to manage the risk: Quality control existing products.

The internal control is very broad. How do we ensure all products are tested? Since we can't check every item, what happens if the supplier changes the specification without our knowledge?

We will therefore consider such 'internal controls' as level 2 objectives (sub-objectives) and we identify the level 2 risks threatening those.

3.5 Subsequent level objectives and risks

Using interviews, risk workshops and the other methods we have covered, the mind map (or spreadsheet) can be expanded until the internal controls become identifiable tasks that we can check as part of an audit. Controls may become identifiable after the first, second or third level risks. See the mind map (appendix D) or RAU spreadsheet for examples.

This is the advantage of using a mind map; it is flexible and allows changes to be easily made as we experiment with identifying objectives, risks and controls. There may be a level at which it is better to stop and use audits to identify detailed risks and controls.

The other advantage of using a mind map and spreadsheet is that they are easily updated. Thus we do not need to record all the organization's risks in one operation but can work in stages.

As the mind map becomes very large, it has been split, with links to subsidiary mind maps. The spreadsheet has also been split, although sorting is easier if it is kept together

3.6 Strategies

As was noted in 3.2, the first level objectives include, ' Set up a strategy to deliver the objectives'.

For example the level 1 strategy could include targets such as:

- Grow the existing business profit by 2% in real terms
- Establish a web based new business
- Monitor new technologies with the intention of exploiting some

The strategy should set the tone of the organization and incorporate the expectations of legislation and other requirements such as COSO. For example:

- Reinforce expectations of integrity and ethical values from employees and outsourced operations by continued publicity of the organization's 'Standards of Conduct'.
- Establishment of a 'Whistleblower' function
- Use only suppliers who trade ethically

The first objective at level 1 is to define strategies which deliver the other level 1 objectives. The level 1 risks threatening this objective include:

- Company does not achieve stakeholder objectives (the company's strategy doesn't include the objectives of the stakeholders (investors))
- Opportunities are missed (the company fails to grow because it doesn't take advantage of its market position).

The sub objectives (level 2) which act to manage these risks are generally:

- Decide on a strategy to deliver the stakeholder objectives (that is, determine the stakeholder's objectives and ensure the strategy contains targets to deliver them)...
- Communicate the strategy.
- Deliver the strategy.
- Support the strategy by providing resources.

There are level 2 risks which threaten these objectives, such as 'The strategy is not financially justified', which affects the first objective. There are then controls, or level 3 objectives, which manage these risks. The spreadsheet provides examples.

The level 2 and 3 objectives and risks are somewhat contrived, artificial and probably too complex! But apart from this:

- We have identified the risks threatening the first primary objective.
- We have identified some of the controls necessary to manage the risks.
- At least we have a methodology to criticize and improve.

Each of the first level objectives noted in 3.2 will require a strategy and support to deliver it. The spreadsheet provides examples...

3.7 Accounting systems

Risks that threaten a company's objectives will differ depending on its operations (e.g. retail, manufacturing, and banking). However, risks threatening a company's financial accounting systems (accounts payable, fixed assets, general ledger) are likely to be similar, hence the wide availability of audit programs covering these systems.

I tried using some of these programs to speed up thinking about the risks but very few are based on identifiable risks and they are inconsistent. So I started from the basics:

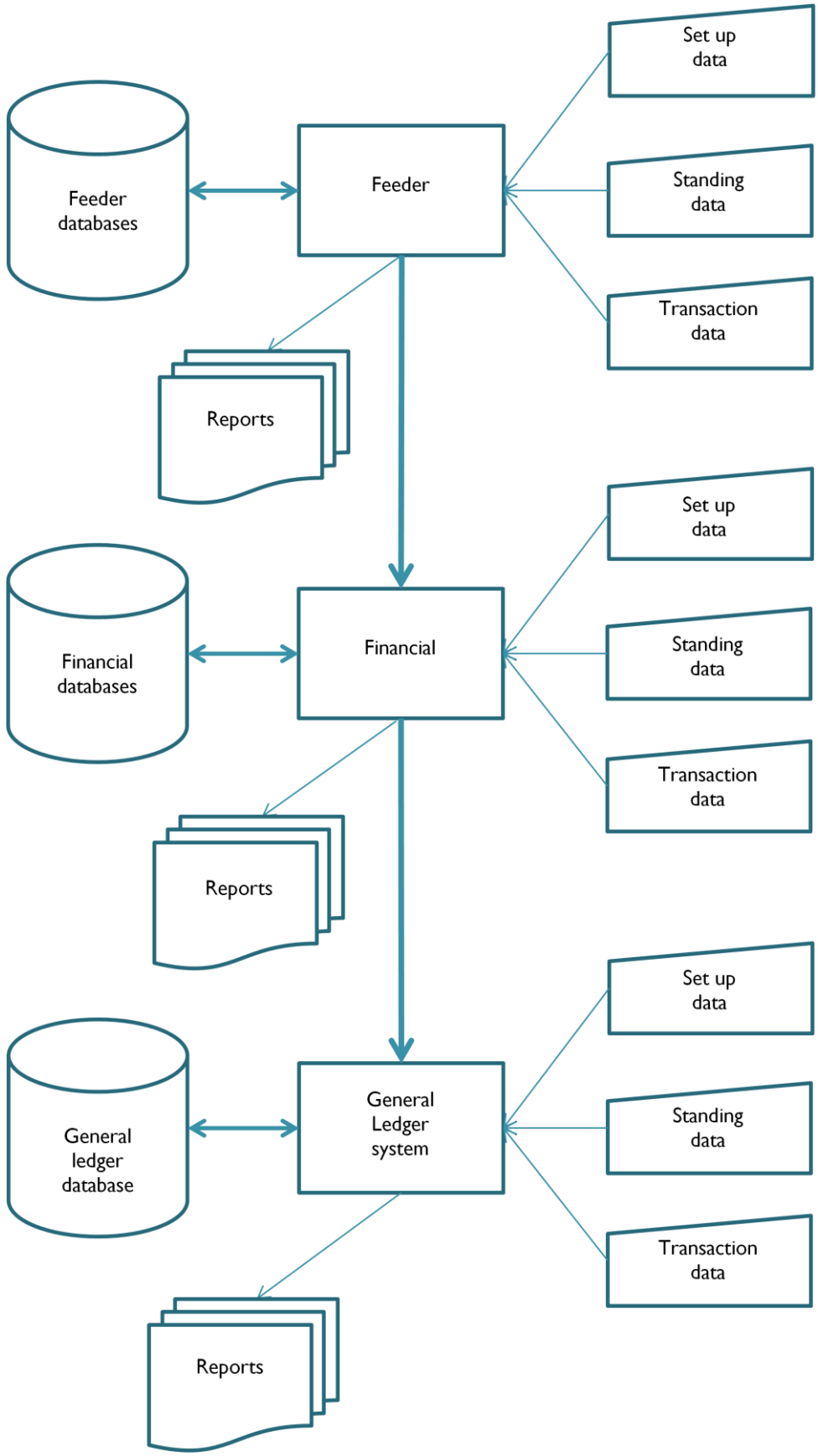
- I assumed computer systems are used - although the risks can be applied to manual systems.
- I assumed the basic structure of systems shown in the diagram on a following page:
  - Feeder systems (sales ordering, purchase ordering, time recording and warehouse stock control) passing data to...
  - Accounting systems (accounts payable, accounts receivable, payroll, fixed assets, stock accounting) passing summarized data to a...
  - General ledger from which management and financial accounts are prepared.
  - (I've ignored the possibility that the GL might feed into a financial consolidation and reporting package).

I then considered the elements of these systems:

- Input:
  - Set up data: input when setting up the system (accounting calendars, currency to be used, account code structure). Rarely changed.
  - Standing data: Any data which is not transaction data! Supplier addresses, employee names, tax rates. May be changed frequently or very rarely.
  - Transaction data: forms the basis of the accounting information (sales and purchase invoices, receipts of cash and stock, payments to suppliers and employees).
- Account balances (accounts payable (creditors), accounts receivable (debtors), fixed assets, stock, bank and cash) which result from the input.
- Programs: computer coding which handles and manipulates the data.
- Databases: computer tables holding the data in computer storage.
- Output: reports (screen or paper based).
- Output: data passed to another system (order data or payments).

Each element has its own high level risks, which we can determine and use to drive out the specific risks for each system together with the associated controls. Appendix D shows these typical risks and controls. They are not complete and require additions, depending on the accounting system being audited. Tests have not been suggested for all controls.

A flow chart showing the typical processes for financial systems is shown below.


Set up data
Feeder databases
Feeder
Standing data
Transaction data
Reports
Set up data
Financial databases
Financial
Standing data
Transaction data
Reports
Set up data
General ledger database
General Ledger system
Standing data
Transaction data
Reports

3.8 The ORCR

So after many months of interviews, risk workshops, accounts examination and reading of legislation and standards, we have recorded many of the opportunities and risks which benefit/threaten the organization's objectives and have identified controls which should exist to manage them. All of this is on the mind map. Nobody said it was going to be easy!

We need the register to be in a form which we can sort and add further information, so the mind map (if used) has to be exported to a spreadsheet or database. If this isn't possible it will have to be copied manually.

We will now have a spreadsheet with a line for each control and columns for objectives, risks and controls. This is known as the Objectives, Risks and Controls Register (ORCR) (https://www.internalaudit.biz/files/rau/rbiacompilationrau.xlsx).

The mindmap is also included in this workbook. The mind map was created using VisiMap from CoCo Systems (www.coco.co.uk/).

3.9 Lessons learnt

1. Risks and controls are appearing in a different order to that which arises from looking at processes and systems - as internal auditors traditionally view the organization. This isn't surprising as processes are vertical in nature, for example purchases moves from ordering, to invoice approval to payment. However the organization also works horizontally across processes, for example: research new products; purchase; stock in warehouse; distribute to stores; sell.
2. Since the 'Support' objective is on every level, some objectives, risks and controls may be difficult to place. For example IT support applies to objective levels 1, 2 and 3. In practice level 1 IT objectives and risks will relate to the overall governance of IT; level 2 will relate to IT support of the ongoing business and developments, including IT projects; level 3 IT objectives will relate to specific functions such as the general ledger.
3. The risks and related controls determined at the start of setting up the ORCR will be almost all related to the business operations and not the processes which the business uses. The risks resulting from processes (cash sales, accounting for fixed assets) are more likely to be identified when carrying out audits, or examining previous audit files.
4. Objectives and risks can be interchangeable, just by using different phrasing! For example, 'Communicate the strategy' is an objective, whereas 'Inefficiency results from the strategy not being communicated' is a risk! It may not matter, provided we remember that our ultimate aim is to identify the risks which threaten our objectives and the controls necessary to manage them.

4 Managing opportunities and risks

4.1 Introduction

We have now identified many of the opportunities benefitting and risks threatening our objectives. The next stage is to document the responses to opportunities which will maximize their benefits and to risks which should minimize their threat to a level the board considers acceptable.

So at this stage we need to:

- Set up a system which measures the threat of the risk or the benefits of an opportunity.
- Score the opportunities and risks using this system.
- Set a risk appetite so we can so that we can identify those opportunities and risks we need to manage.
- Identify an owner of the opportunity/ risk, who has the responsibility of ensuring it is managed with internal controls.
- If necessary, deciding if the internal control is so important that its operation needs monitoring.

4.2 Risk scores

Each risk requires scoring for consequence and likelihood, before and after internal controls. Details are given in Book 1, 'Risk based internal auditing - an introduction' in www.internalaudit.biz. The table of scores from that book is 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.

4.3 Opportunity scores

Opportunities usually arise from decisions, so how do we score these? The audits will be concerned with the decision making *process* not the decision itself, where simple scoring can't be used. Therefore the consequence of the decision will need to be scored together with the likelihood that it will *not* deliver the opportunity (that is the reverse of the risk likelihood). For example, the decision making process at board level would have a score of 5 for consequence and 5 for likelihood if there were no processes to manage its successful delivery. If controls such as financial modeling and training existed then this likelihood score would reduce but not the consequence. The decision making process for a new credit customer would score less for consequence, since its impact on profitability would be less.

4.4 Risk Appetite

It is the Board's responsibility to determine what risks are not acceptable by deciding what risk score is unacceptable. (Book 1 provides more details.) Knowing the risk appetite we can then select those inherent risks which must have responses to bring the residual risk to below this risk appetite. It is these risks we will need to build into the audit plan.

Since opportunities have been scored using a similar method to risks, the risk appetite should apply.

4.5 Risk ownership

Allocating an opportunity or risk to an owner is essential, as it is this job holder who is responsible for ensuring the control(s) manage the opportunity/risk, are operating, changes to the opportunity/risk is notified to the 'risk guardian'. Opportunity/risk owners are identified using a functional hierarchy of the organization. For opportunities, the owner could be the project manager tasked with delivering the opportunity.

The operation of some controls may need monitoring by a senior manager, such as signing the bank reconciliations. The job holder needs including on the spreadsheet. An example hierarchy is included with the spreadsheet.

The advantage of including the risk owner is that 'Control self-assessments' can be generated from the spreadsheet in order to obtain assurance from the risk owner that the control is operating.

The risk owner needs to agree those risks allocated to them and be involved in the scoring.

4.6 Internal controls

Ideally, the opportunity/risk owner should be able to detail the controls which are a response to the inherent opportunity/risks and to score the resultant residual opportunity/risk. Internal Audit may provide assistance here as a 'trusted advisor'.

5 Planning

5.1 Risk and Audit Universe

We now have an ORCR which lists the objectives of the organization, split down so that we can identify individual risks and controls. We are now at chapter 6 of Book1 (Compiling the risk and audit universe). The next stage is to form the Risk and Audit Universe by allocating each opportunity and risk to the audit which will check the proper operation of the response to the opportunity/risk. In some cases, a risk may be ignored, for example if a decision has been made to accept the risk or if the inherent risk is below the risk appetite.

It is at this point we turn the ORCR, which is the responsibility of the organization's management, into a document which forms the basis of practical audit field work - The Risk and Audit Universe (RAU).

5.2 Deciding on audits

What is an audit? From our definitions, we can say that an audit is a series of investigative tasks from which we can make an objective opinion about whether the organization will achieve its objectives in the areas being audited.

As with any operation, the ideal method of working is to maximize the output while minimizing the resources necessary. In practice this means:

- Concentrating on the highly scored inherent risks.(Not the residual risks, since these are scored after taking into account the controls we are checking!)
- Carrying out an audit where the departments involved are physically close together, in order to minimize travelling time.
- Involving a limited number of staff and managers in the departments concerned, in order to minimize the number of meetings while building up trust between managers, staff and the auditors.
- Involving a limited number of processes. This allows the auditors to understand the processes in depth, identify risks not identified by the management, carry out efficient testing - using both manual and computer methods.

It is therefore beneficial to group the risks so that the internal controls mitigating them can be checked efficiently in one audit. The identification of risks with 'owners' and 'processes' is a good start, since this will generally group risks such that they can be audited efficiently. However, audits (such as purchases) will probably involve several owners.

In the US, we will need to ensure sufficient audit work has been done to complete the COSO 'Overall assessment of internal control template' and SOX requirements.

So we now need to allocate risks to audits. The methods are covered in Book 1, section 6.3. The work done in an audit is detailed in Book 4 (the Manual).

5.3 Processes

Processes reflect objectives, since processes are the tasks which deliver the objectives. Two processes will usually appear at each level in the hierarchy (see spreadsheet):

- *Establish strategy*. Each process, such as 'purchase goods for resale' should have a strategy which would include development plans (new products) and reinforce the culture and values set by the organization's top level strategy (buy only from ethical suppliers).
- *Support organization*. Each process will need supporting, for example staff should be recruited, trained and developed, particularly in decision making.

5.4 Functions

Functions organize the staff to operate the processes to deliver the objectives. They will bear some resemblance to processes but typically some functions will operate parts of several processes for example purchasing for resale covers: purchasing, stock, AP and stores processes.

This is nothing new; it is encountered in systems auditing!

5.5 Next steps

Now that the ORCR is established, the other books provide the next steps:

Book 1 - An introduction details

- how to set up an audit plan (chapter 7)
- the stages of an audit (chapter 8) with example working papers

Book 4 - The manual provides ideas about working papers. It is based around the audit of accounts payable noted as 205 on the 'Maintain profits RAU' spreadsheet.

(Book 3 - Provides some ideas about implementing RBIA.)

6 Appendices

TOPIC		Original*
Interviewing tips	A	This document
Running a risk workshop	B	This document
Level 1 objectives and risks mind map	C	This document
Expanded mind map example	D	This document
Typical accounting system risks and controls	E	This document
Audit tests for decision-making	F	This document

6.1 Appendix A - 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 opportunities and 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 the biggest opportunities and risks arising in any organization come from the decisions made. Ask about the interviewee's decision-making processes using the questions in appendix F as a guide.
- 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.

6.2 Appendix B - 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.

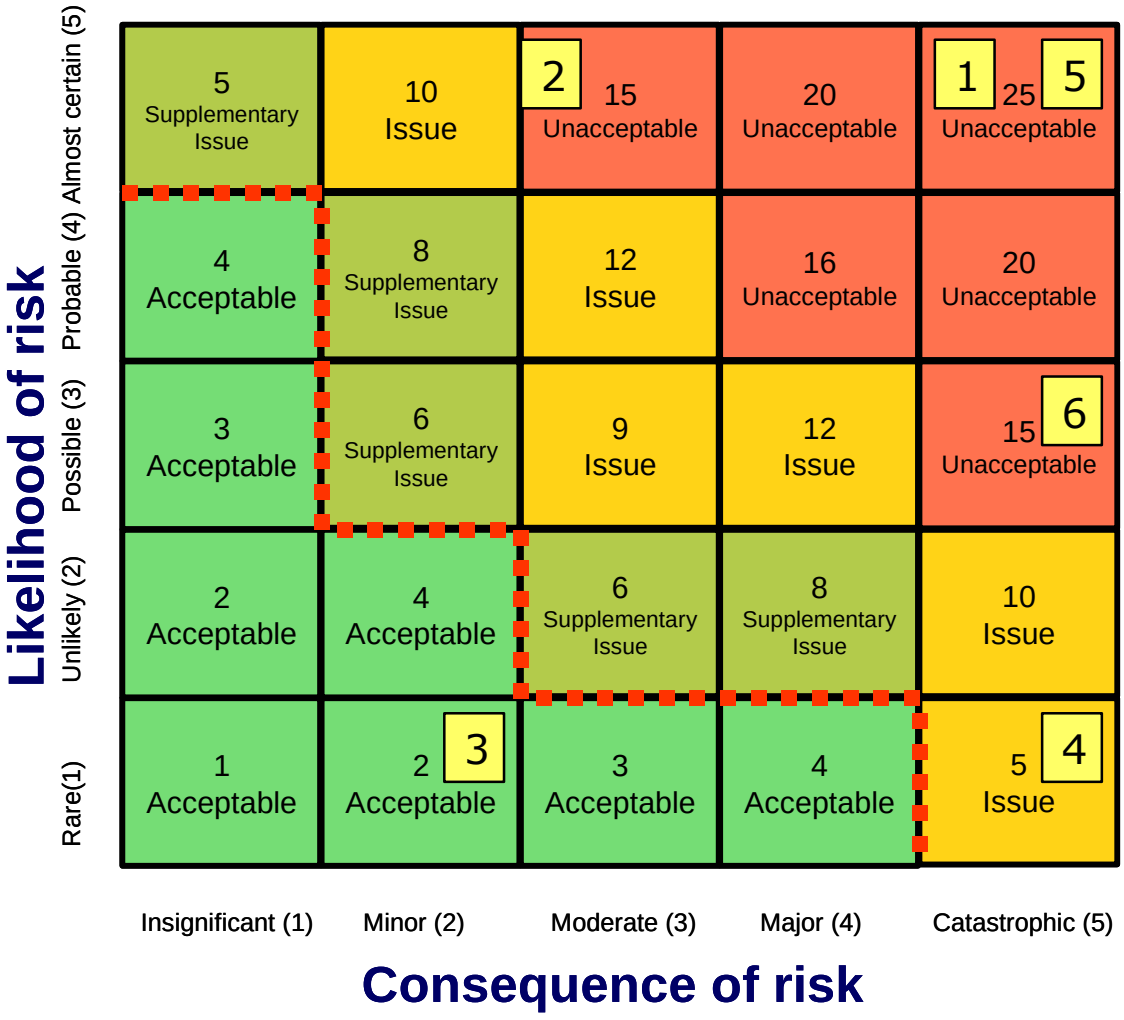
Preparation:

- 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 opportunities and risks. They must be visible to the entire meeting.

- For each objective, ask members of the team to shout out the opportunities which might benefit and 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 an opportunity or risk is not understood by all. Don't worry if one opportunity/risk affects more than one objective, or you can't easily allocate a opportunity/risk to an objective, the important task is to record the opportunity/risk once against any relevant objective. This risk identification takes about an hour.
- When wording opportunities and risks, try not to make them just the failure to deliver a process. For example the risk hindering 5.4 "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 opportunities and 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.

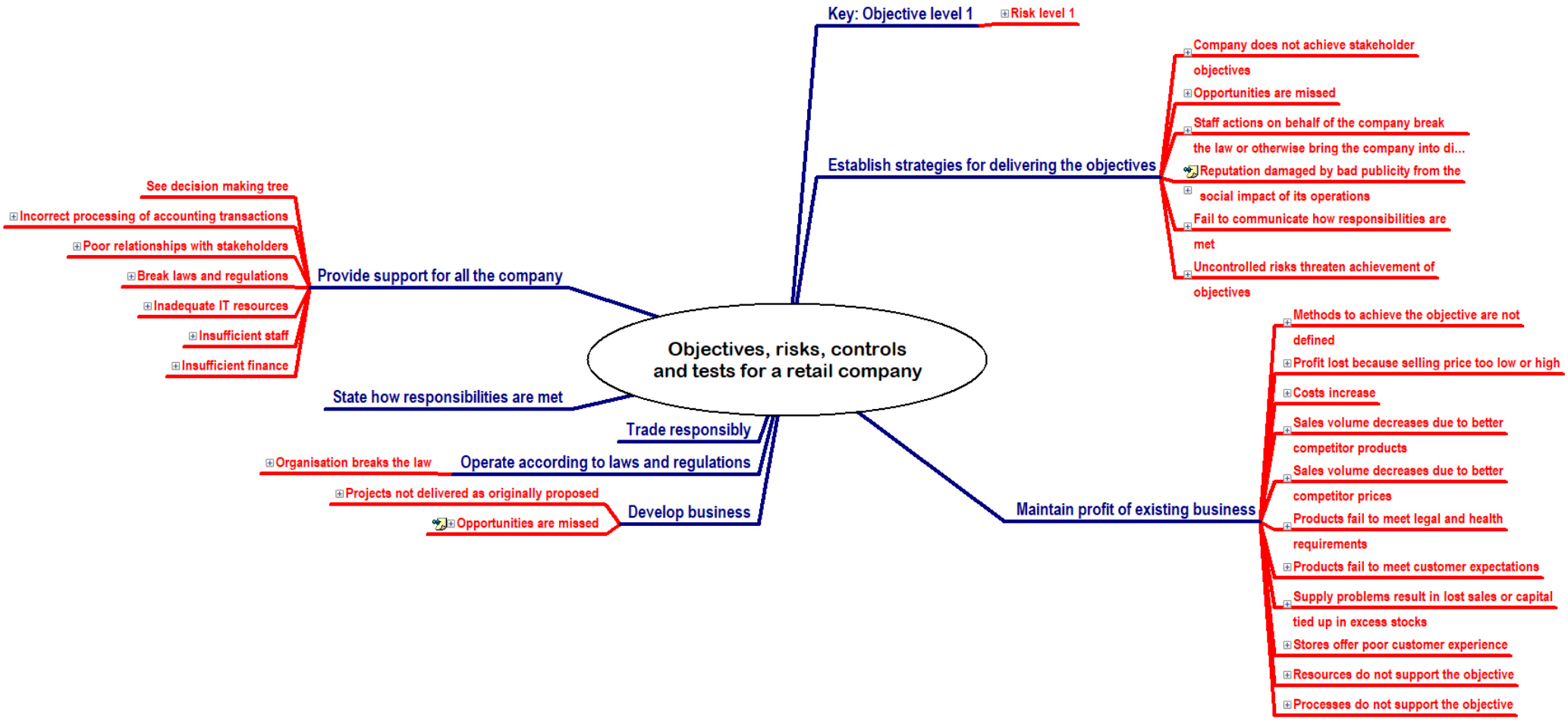


- Draw two axes on a large piece of paper (I use four flip chart sheets stuck together) and label them as below. If you are really sophisticated you can have a large laminated sheet set up, with the most significant risks highlighted in red (see below). You may also be able to use an interactive white 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! Use Post-it notes of different colours for opportunities and risks.
- 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 opportunities would benefit, and risks which threaten, the achievement of 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 opportunities and risks.
- You will have taken about two hours to reach this point and everyone is exhausted. STOP NOW!

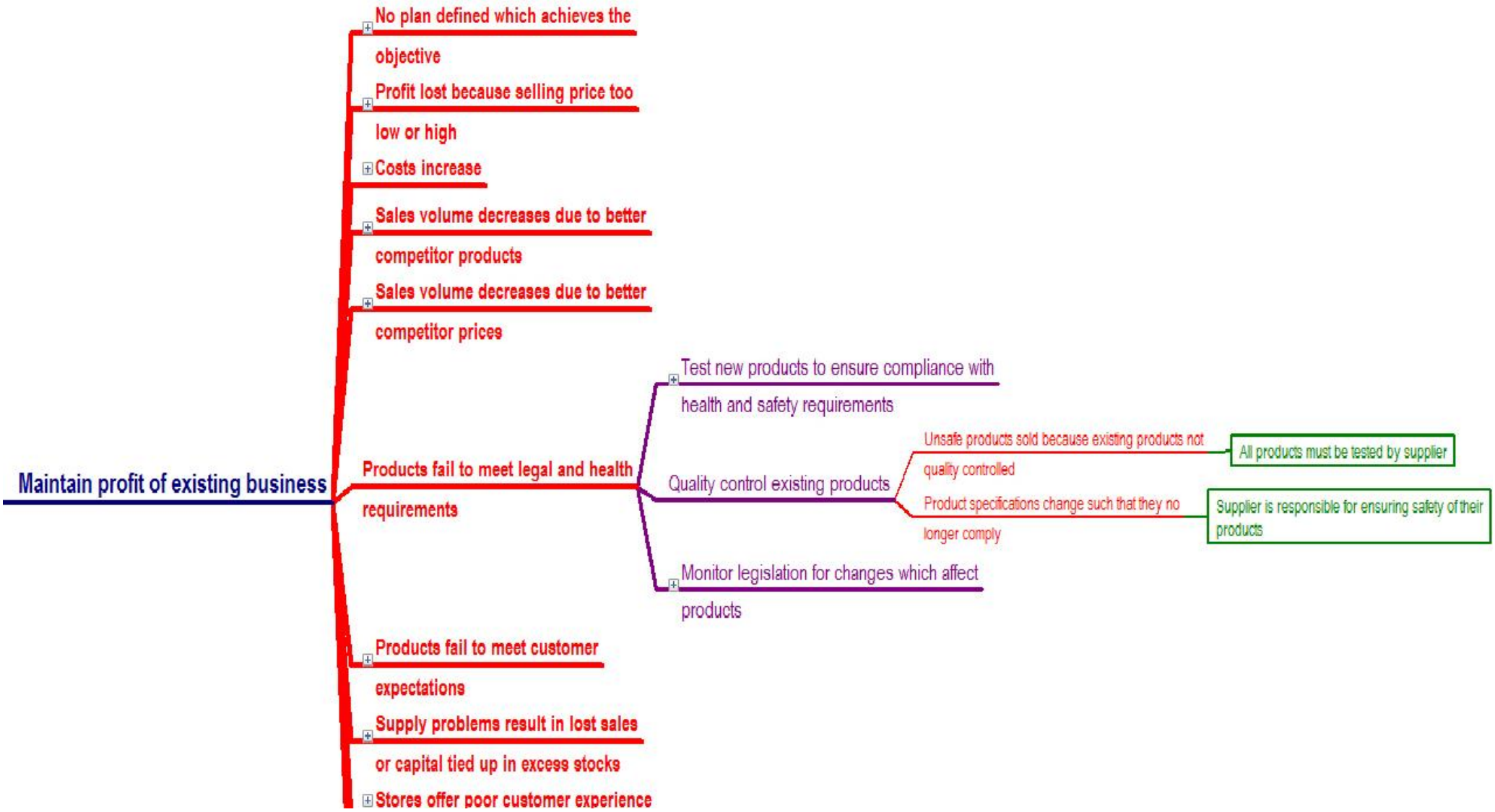
Assigning risks

- The next stage is to consider:
  - How opportunities which might present themselves can be used to maximize their value.
  - 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.

6.3 Appendix C - Level 1 objectives and risks mind map



6.4 Appendix D - Expanded mind map example



6.5 Appendix E - Typical accounting system controls

Objective 3	Risk Level 3	Example control	Example test
Data used for set up was complete, accurate and complied with regulations	Data supplied was incorrect	Use data from a trusted source	If relevant, check any changes which have been made to set up data back to an authorized source
	Data was input incorrectly	Check data on system to data on source	If relevant, check any changes which have been made to set up data back to an authorized source
		Run tests to check set up data is correct	If possible use CAATs to check set up data is correct
Data used for standing data was relevant, complete, accurate and complied with regulations	Data supplied was inaccurate	Use data from a trusted source	Check a sample of standing data back to source
	Data was input incorrectly	Check data on system to data on source	Check a sample of standing data back to source
		Run tests to check set up data is correct	Run CAATs to check standing data is correct
Data being used to update standing data is relevant, complete, accurate, timely and complies with regulations	Data supplied is inaccurate	Use data from a trusted source	Check a sample of standing data back to source
	Data is input incorrectly	Check data on system to data on source	Check a sample of standing data back to source
		Check output is correct	Run CAATs to check output is correct (or check an output sample manually). E.g. correct depreciation calculation
	Data supplied is incomplete or not supplied	Check all required data fields on system are completed	Confirm computer edit checks (or manual checks) ensure completeness of data
		Exception reports to highlight incorrect or missing data	Run CAATs to check for missing data (or check an output sample manually)
	Data is input at the wrong time	Use a checklist and timetable	Examine written procedures to ensure correct cut-off
		Use a checklist and timetable	Examine checklists and timetables, or other documentation which ensures objective is achieved
	Data does not conform to regulations	Check data source conforms to regulations (both company and legislation)	Run CAATs to select data and check this conforms to legislation (or check an output sample manually)
		Set up computer edit checks to highlight suspect data, such as incorrect tax calculations)	Observe input of standing data to ensure incorrect input is rejected, or warnings issued
		Data to be approved by tax or legal specialists, if necessary	Where data should have been checked by specialists, look for evidence of approval
	Malicious/fraudulent data set up	Restrict access to input screens	Obtain names of staff, including IT staff, who have access to the system being audited. Check that access is appropriate and kept to that which is necessary
		Duties for updating data are divided so as to ensure no-one has responsibility for the entire transaction cycle	Ensure that duties are divided between staff such that no-one can set up fraudulent data without it being detected by a second person

Objective 3	Risk Level 3	Example control	Example test
		Exception reports to highlight unusual transactions	Obtain exception reports, or run CAATs, to highlight transactions such as disposal of high vale items
		Training of staff to include notifying senior management of any suspicious activity	Check that formal procedures exist for notifying senior management of any suspicious activity and that these are included in training
Transaction data being used to update balances is relevant, complete, accurate, timely and complies with regulations	Data supplied is inaccurate	Edit checks to report inaccurate data	
		Use data from a trusted source	
	Data is input incorrectly	Edit checks to report inaccurate data	
		Check data on system to data on source	
		Check output is correct	
	Data supplied is incomplete or not supplied	Feeder systems (e.g. purchase orders) should provide all necessary data	
		Edit checks to report missing data	
		Check all required data fields on system are completed	
		Exception reports to highlight incorrect or missing data	
	Data is input at the wrong time	Edit checks to detect data input into wrong period or with incorrect dates	
	Data is input at the wrong time	Exception reports to highlight data posted in wrong period	
	Data does not conform to regulations	All items should have passed through procedures which checked they complied with tax, company and statutory regulations	
		Check data conforms to regulations (both company and legislation)	
		Set up computer edit checks to highlight suspect data, such as incorrect tax calculations)	
		Data to be approved by tax or legal specialists, if necessary	
	Malicious/fraudulent data set up	Restrict access to input screens	
		Division of duties	

Objective 3	Risk Level 3	Example control	Example test
		Exception reports to highlight unusual transactions	
		Training of staff to include notifying senior management of any suspicious activity	
The balance total agrees with that in the general ledger	Data input directly into GL without a system transaction	All data which affects the system balance to be input via the system	
	Data not transferred from system to GL	Month end check of balances formally noted on a checklist	
		Daily checklists (or as appropriate) to ensure data is transferred	
	Timing differences between system and GL input	Month end checklist to ensure all transactions transferred from subsidiary ledgers to the GL	
	Items making up the balance cannot be identified with authorized transactions	Only complete transactions to be posted (e.g. invoices, fixed assets)	
		No adjustments (such as journals) should be made without a clear audit trail to supporting documents	
		Periodic check of balances to ensure all items are related to proper transactions	
	Items making up the balance are overdue	Exception reports to be produced showing overdue items	
	Items making up the balance don't comply with regulations	All items should have passed through checking procedures which checked they complied with tax, company and statutory regulations	
Output data is relevant, complete, accurate, timely and complies with regulations	Output data is not relevant	User testing of reports to ensure they achieve their objectives	
	Output data is not relevant	The decisions to be made on receiving the report are defined	
	Output data is incorrect	User testing of reports to ensure they achieve their objectives	
	Output data is incorrect	Exception reports to highlight data outside expected values	
	Output data is incomplete	User testing of reports to ensure they achieve their objectives	

Objective 3	Risk Level 3	Example control	Example test
	Data is output at the wrong time	Exception reports to highlight data outside expected period	
	Output data does not conform to regulations	User testing of reports to ensure they achieve their objectives	
		Exception reports to highlight data outside expected values	
The database is secured against alteration, other than by permitted transactions	Unauthorized alterations occur	Password restricts access to system	
		IT controls prevent direct access to files	
		IT system logs access to files	
Malicious corruption is prevented	Computer virus corrupt database	IT apply latest virus databases immediately on receipt	
Corruption by malfunctioning IT systems is prevented	Malfunctioning hardware or software corrupts data	Database files are backed up daily	
		IT checks warn if databases become corrupted	
	Incorrect IT procedures result in incorrect restoration of files	Procedures to be used for restoring backed up files are documented	
Physical damage to hardware is prevented	Hard drives and other storage media damaged	Computer equipment is in a room with restricted access	
		Computer room has automatic fire extinguishers	
	Hard drives and other storage media stolen	Computer equipment is in a room with restricted access	
		Computer room is on a site with restricted access	

6.6 Appendix F - Audit tests for the decision-making process.

Control to maximise opportunity	Audit test
Set objectives	
Governing body defines top level objectives.	Is there a list of objectives approved by the governing body?
Top level objectives communicated to all job holders	Are objectives communicated to all job holders, for example through an intranet?
Acquire information	
Information is gathered and presented in such a way as to ensure any decisions required are identified as soon as possible	Is all relevant information which is necessary to make decisions gathered as soon as possible? Is it used to generate forecasts which might trigger decisions? Is the information accurate?
Information is summarised and processed as necessary before being communicated.	Is the information communicated to the job holders responsible for making decisions as soon as it is available? Do the decision makers check the information on receipt and act as necessary?
Make value adding decisions	
Information received triggers an appropriate response	Is the information presented in an easily understandable form such that the need for a decision is clear? Does the job holder receiving the information understand their responsibility for making a decision?
Understand what the decision has to achieve	Has the decision to be taken been summarised in a few sentences? Has this summary been circulated to all involved?
Determine by when the decision should be delivered	Has a full timetable been drawn up, showing the stages of decision making and the action required to deliver it? Has a critical path analysis been derived to understand the vital stages of the process?

Identify all possible options which might deliver the desired outcome	Have all job holders who could possibly provide relevant information and guidance been identified and involved in determining the possible options? Where appropriate, has the range of options available to the decision maker been predefined (e.g. value limits, limits on possible action)
Determine the advantages and disadvantages of each option	Has all relevant information been obtained for each option? Has the information been assessed for accuracy? Where appropriate, has financial modelling been used for each option? Has the impact of each option been considered together with any action which might be necessary to manage this impact?
Decide on the best option	Has the best option been chosen, based on the advantages and disadvantages of each? Has the final decision been the subject of an independent review? Has the reason for choosing the option been documented?
Identify the actions necessary to deliver the decision	Have all actions been identified? Have these actions, with timings and responsibilities been incorporated into an updated plan? Has one person been charged with co-ordinating the action so that the decision is delivered on time and within budget?
Communicate the decision made and the actions required to deliver it	Have the job holders charged with taking action been informed of their responsibilities, including targets?
Monitor progress of the plan	Have targets been incorporated into formal appraisals? Is actual progress against the plan regularly monitored? Is progress against the plan communicated to relevant job holders, especially if delays are occurring?

Prepare a report on lessons learnt	When the decision has been delivered (or not) has a report been prepared analysing what worked well and what could be improved? Have lessons learnt been fed into training?
Job holders understand what they can decide	
The governing body approves in writing the overall policy for decision making, usually expressed in monetary amounts	Obtain written copy of board paper which describes policy for decision making and quantifies this for different job grades
Senior management interprets policy and defines authority limits for each job	For jobs relevant to the audit, examine documents which define authority limits. Examine job descriptions. These should state the objectives of the job; decisions it is required to make; limits over those decisions.
Job holders know how to decide	
Induction training is provided to all job holders moving into a new job	Examine induction training programs to ensure they cover the contents of the job description
Training provided for all job holders	Confirm all job holders have been trained in making the decisions appropriate to their job. Where jobs involve decision-making which must be in seconds, ensure training involves 'real life' situations. Use specialists in the audit team as necessary. Check training includes the need for job holders to recognise opportunities and threats to the organisation's objectives and how to communicate these.

7 Version control

Version	Date Added	Changes made to previous version
Draft	14 October 2013	Added more on finding objectives. Added appendices and accounting system controls.
Draft	20 October 2013	More information on determining objectives and risks
1.0	27 January 2015	Added more chapters
1.1	4 March 2015	Section on Organizing risks amended with more explanation. Functions and processes added. Minor amendments, including more details on strategies, processes and functions.
1.2	19-May-2015	References to 'risk register' changed to 'ORCR'
1.3	26-May-2015	Reference made to Book 4
2.0	5-Jun-2020	Updated to include opportunities and decision making. Change emphasis for risks to objectives.