Risk-based Auditing

PHIL GRIFFITHS

GOWER
CHAPTER 1

What is Risk-based Audit?

The Internal Audit identity crisis

Let’s face it, if you are reading this book, you are probably either already an auditor, preparing to become one or responsible for managing or overseeing the function. The other possibility is that you are considering a role in Internal Audit – if this is the case I hope to be able to whet your appetite and show you what a wonderful opportunity it brings.

Whichever category of reader you are the first major bridge to be crossed is the identity of the function.

I was to learn that we tend to meet any new situations by reorganising – a wonderful method for creating the illusion of progress

This quote by the Roman Caius Petronius in AD 66 illustrates the dilemma for Internal Audit.

Internal Audit has seemingly attempted a number of changes in approach over the years, but have any made a real difference?

Is Internal Audit seen as the ‘White Knight’ charging in full armour, past cheering throngs of well-wishers to rescue the damsel in distress or the ‘Lady with the Lamp’, splendid and serene, tending to the ranks of wounded in the Crimean War without a thought for her personal well-being.

Probably not.

It is more likely that an auditor may be seen, to use the old joke, as the team that comes in after the battle and bayonets the wounded.

The role still has somewhat of an identity crisis. Risk-based audit offers some, if not all, of the solutions.

In the following chart I would like to pose a question to you to illustrate the point.

Please pick the one creature which you believe best describes the role of Internal Audit in the eyes of the Chief Executive or Directors of your organisation. Try and put yourself in their shoes. If you asked them the same question, what do you believe their answer would be?

Let’s analyse the most likely responses:

• Dinosaur
  If this is the perception, you have a major task ahead. You need to move quickly; otherwise you may become extinct.

• Snake
  The snake in the grass, waiting to trap the unwary, is a very common metaphor for the function in management’s eyes.
• Praying Mantis
  This insect looks reverent and calm (the stance looking as though it is at prayer) but if a
tasty morsel passes it, it is ready to strike and become a ‘preying’ mantis. Does Internal
Audit give out these vibes? Outwardly innocent but a menace in disguise.

• Bee
  Buzzing from flower to flower not staying long in one place and a sting in the tail if
things get really tough. Better than the dinosaur, praying mantis or snake but still
probably not quite how Internal Auditors would like to be seen.

• Koala
  Let’s be realistic, you are never going to be regarded with as much affection as the cuddly
koala bear.

• Donkey
  Dependable, not afraid of hard work and has to carry many burdens – maybe not such
a bad comparison.

• Ant
  A fantastic teamworker but small and easily trodden on.

• Dog
  Reliable, faithful and if it is a guard-dog, looking out for the business – a safety and
comfort provider. Maybe quite a good metaphor – unless you are seen as a terrier
snapping at the heels.

• Lion
  Strong, respected but can be very fierce and intimidating. Much better than the snake
but probably not quite as you would wish to be seen.
• Dolphin
   Super-intelligent, sleek, fast and loved by everyone. It would be very good to be thought of as a dolphin. This is a very good goal for Internal Audit, although I am not sure if you will ever be loved by everyone.

• Eagle
   The very best metaphor for modern Internal Audit. The eagle flies majestically across its domain, able to watch over its environment and take everything in and when necessary can swoop down and deal with issues.

The risk-based audit approach is the tool you need to ensure that you are increasingly regarded as the eagle or the dolphin.

Definitions and outline

So what is risk-based audit? It is a process, an approach, a methodology and an attitude of mind rolled into one. The simplest way to think about risk-based audit conceptually is to audit the things that really matter to your organisation. Which are the issues that really matter? Probably those areas that pose the greatest risks. What else would you really want to review? If your organisation has already identified its key risks then you already have the basis for risk-based auditing. Clearly, if risks have not been formally identified and assessed then there is a real opportunity for you to work with management to help create this information.

The second way of looking at risk-based audit is as a process. Traditionally audits begin and end by looking at controls, often regarded as the main expertise that the function has. The problem with this approach is two-fold.

Firstly, management do not really understand controls, which can be an alien concept for them. If they do understand the nature of controls they tend to consider the need for more controls as an unnecessary additional burden.

Secondly, it is unlikely that your Internal Audit function is an expert in control. Can you really say that you understand the controls in all aspects and all activities within your business? It is therefore necessary, if you are going to demonstrate your eagle-like qualities, to be able to talk to management in a language they understand and appreciate. To fully engage management you need to talk to them about something that is important to them. If you start by discussing their objectives, what they need to achieve and how this is measured you will attract their attention.

Having created the common ground (and it is preferable if you have first given some thoughts to the objectives in the area under review before the meeting), you can now go on to discuss the threats to the achievement of those objectives, the barriers to success; these are, of course, the risks.

Again management should be able to elucidate many of the risks or threats, but theoretically, if you have tried to anticipate the types of threat beforehand this will act as a positive spur.

Having created an understanding of the objectives and risk you can then discuss the risk appetite, the boundaries set by senior management (by authorisation limits and so on) or, indeed locally, the limits beyond which the management of the function to be audited will not venture (or is advised not to go) in risk-taking.
The next stage is then to discuss the processes in place to mitigate the risks already identified and those that appear on the horizon and the areas of concern or opportunity in relation to those processes.

You are now, of course, talking about the controls, but rather than doing so in isolation you will be discussing them as part of the full management process and should receive a much more positive response as a result.

The essence of risk-based audit is therefore customer-focused, starting with the objectives of the activity being audited, then moving on to the threats (or risks) to achievement of those goals and then to the procedures and processes to mitigate the risks. Risk-based audit is therefore an evolution rather than a revolution, although the results obtained can be revolutionary in their magnitude.

The chapters that follow expand these principles into a full process, explain the attitudinal changes and the broader range of skills required together with the tools and techniques necessary to adopt the process and to become a world-class Internal Audit function.

The challenges for Internal Audit

Figure 1.2 Do you recognise yourselves? Are auditors fighting the good fight? What could the big ‘C’ word signify in relation to the audit role?

- **Control**
  Ask auditors their prime area of expertise and many will say ‘Control’. Can you honestly say that you are an expert in all aspects of your organisation’s operations? I doubt it. Why then is Internal Audit obsessed with control?
Compliance
This is an important aspect of the traditional audit role. It is still very important today, getting the basics wrong can spell disaster for organisations, but should compliance be the main focus of the Internal Audit role? Our continuing research with Chief Executives would clearly indicate that this is not the case.

The question was asked as to the prime focus of the function. The respondents had to pick the approach that was primarily followed.

Prime focus of the function
Bi-annual Chief Executive’s survey

<table>
<thead>
<tr>
<th></th>
<th>2000 Percentage</th>
<th>2002 Percentage</th>
<th>2004 Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Business risk orientated</td>
<td>40</td>
<td>72</td>
<td>89</td>
</tr>
<tr>
<td>Financial systems based</td>
<td>23</td>
<td>7</td>
<td>1</td>
</tr>
<tr>
<td>Operational systems based</td>
<td>20</td>
<td>10</td>
<td>2</td>
</tr>
<tr>
<td>Compliance orientated</td>
<td>10</td>
<td>6</td>
<td>1</td>
</tr>
<tr>
<td>Internal consultancy</td>
<td>4</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Value for money</td>
<td>2</td>
<td>2</td>
<td>0</td>
</tr>
<tr>
<td>Corporate governance</td>
<td>1</td>
<td>2</td>
<td>6</td>
</tr>
</tbody>
</table>

Compliance, as can be seen, is increasingly unlikely to be the prime focus for Internal Audit, with only 1 per cent of organisations who responded adopting this as the primary approach.

As you can see, the prime focus is very definitely focusing on the key risks. This is not to say the other processes are not important, but they are unlikely to remain the dominant focus.

Conflict
Hopefully Internal Audit does not get into too much conflict with management. Over emphasis on control and the failure to make recommendations that are 100 per cent practical can, however, lead to such a situation.

Challenge
This is definitely a key role for the modern function. You need to question the ‘we’ve always done it that way’ mentality and challenge the status quo. If you do not do so in the course of an audit, who will?

Co-ordinate
Wouldn’t it be useful if Internal Audit co-ordinated its activities with the other assurance provider in the organisation, such as Risk Management, External Audit, Health & Safety, and so on. This would reduce duplication and create more focus. An approach on how to achieve such a co-ordinated approach is outlined in Chapter 8.

Champion
Internal Audit should certainly be regarded as a champion. You have the opportunity to look right across the organisation and identify opportunities and good practice. Sharing such ideas is key to success and recognition.
The very best Internal Audit functions are regarded as a catalyst for change, helping the organisation through the difficulties of changing environments, cultures, and so on. Another key catalyst role is bringing people together to discuss areas of concern and opportunity, a best-practice agent.

There are others that you can think of, such as co-operate, convince, conscience, and so on, but I hope that the above have generated an indication of the trends occurring.

The trends

Having suggested that risk-based auditing is an evolution let me attempt to trace this change process. Let’s have a look at some of the trends in risk-based audit. One question to pose is ‘Are you fire fighting all the time or are you able to plan in advance?’ The more fire fighting you do the less likely it is that your organisation is focusing on its key risks. If you are able to link in directly to your organisation’s evaluation of risk, that’s much more effective. The best way to illustrate the transition is to consider the different approaches to Internal Audit.

1 Compliance
   This is where Internal Audit began. It is still a valid approach but is rather limited in its focus, as it tends to concentrate efforts on whether or not the procedures and policies are being adhered to. Is that enough in today’s challenging environment? I would certainly say that it fails to optimise the potential of the Internal Audit activity.

2 Systems-based audit (SBA)
   This is the approach adopted by more modern Internal Audit functions. The approach is predicated on evaluating systems and processes rather than locations or branches. Essentially the SBA is a horizontal rather than vertical approach, reviewing an activity across the organisation and looking for the areas where there are inconsistencies or interfaces are incomplete. Systems-based audit is therefore much less transaction based than compliance, indeed the phrase ‘cradle to the grave’ is often used to describe the process. The approach is to follow a small number of transactions through the system from start to finish to prove its effectiveness.

3 Risk-based audit
   Risk-based audit builds on the SBA approach focusing on the areas of the highest risk to the business and uses a different starting point, business objectives rather than controls. The recommendations made are also risk-evaluated to ensure maximum benefit and buy-in by management.

4 Value for money
   This is the review of a process to determine whether optimum value for money is being achieved and to make profit-enhancing recommendations. This audit approach was used extensively until a few years ago, but seems to have fallen out of favour. I believe that this is an excellent complementary approach to risk-based auditing and would suggest that it should now be a feature of most audits, to assess whether or not the activities
achieve the best value for money in your organisation. Certain audits such as travel costs, mobile phones and other items of corporate expenditure lend themselves particularly well to the VFM approach.

5 Assurance-based audit (ABA)
This is the most recent and some would say the real winner for Internal Audit functions. ABA is using the risk-based approach to co-ordinate all the assurance activities in the organisation to ensure that duplication is minimised, nothing falls between two stools and a co-ordinated assurance position is given to the Board. This topic is discussed in depth later in the book.

Changing the focus

As a way of being able to demonstrate how many organisations’ Internal Audit functions still mainly focus on the traditional issues, let me share some statistics with you. When we ask Chief Executives and Internal Audit functions as to which areas they almost always audit, the answers are quite revealing. The five main areas they say are:

1 Adequacy and effectiveness of accounting controls.
2 Capital expenditure.
3 Physical security of assets.
4 Financial systems.
5 Systems under development.

The first four, as you can see, are the very traditional financially based activities whereas the last one is a much more positive trend, looking at new systems under development to make sure they incorporate controls and effective risk mitigation before the system goes live. The assertion in many studies on the subject is that it is ten times more costly to put in a control after the system goes live than beforehand. So clearly, this is a very positive area for Internal Audit to be involved in. I will return to this topic because some would say that this involvement could compromise Internal Audit’s independence. I don’t share that view and I will explain why later in the book.

When we ask Internal Audit functions which are the areas which they never or almost never audit, we get a very different list:

1 Corporate Planning.
2 Health & Safety.
3 Investor Relations.
4 IT Strategic Planning.
5 Human Resources.
6 Marketing.

As you will recognise, these are much more challenging audits but I would suggest they are the areas that probably represent higher risks to the organisation. Let’s take them in sequence.
CORPORATE PLANNING

This is clearly a critical activity for all organisations. Failure to get this process right could be a road to disaster. So this is a sensible and logical audit to undertake.

HEALTH & SAFETY

It is clearly not sensible to duplicate the work of the health and safety function but is surely very valid to be able to look across the activity to assess its overall effectiveness.

INVESTOR RELATIONS

For those of you in private sector organisations, this is another critical issue; to determine how the organisation’s shareholder relationships are managed. This is an activity which, in my experience, is very rarely audited.

IT STRATEGIC PLANNING

One of the most common reasons, in my experience, for recommendations not being accepted is that management assess that it would require a major system development or IT resource requirement which is not available. Therefore why not have an audit of how the organisation determines its priorities for use of IT resources and systems development.

HUMAN RESOURCES

This is a very important area for any organisation and should therefore be audited. There should not be any area that is off limits for Internal Audit and I would say carrying out an audit of a critical HR management area such as succession planning is usually a very interesting and very important audit. It is one that very few Internal Audit functions carry out.

MARKETING

How many Internal Audit functions would feel confident in going in to do an audit of marketing? This should not hold any terrors as marketing is just a process and auditors’ main area of expertise is process analysis.

Let me illustrate this with a real-life example. In my previous life as Head of Internal Audit for a major retailer, we decided to carry out a review of marketing specifically to assess whether or not the organisation achieved value for money from its corporate advertising spend, particularly television advertising. I went in to meet with the marketing director and he asked a very reasonable question, ‘What the hell do you know about marketing?’ My response was, ‘Not a great deal, but you do!’

The key point I was making is a crucial one for modern Internal Audit functions, as they move into more and more challenging arenas the less likely they will have expertise in that area of the business but, as Internal Audit’s real expertise is process, then any audit should be able to be completed with confidence.

I therefore explained to the Marketing Director that we were intending to review the
process for the measurement and evaluation of marketing spend with a view to assessing its
effectiveness. We therefore embarked on a very different type of audit where we went out
into our stores and we asked the public what had influenced their purchase, had it been the
TV advertising, brochures in magazines or had it been the signage in the stores, and so on.
It was apparent that the marketing function had a bewildering array of often-contradictory
methods of assessing marketing success. As a result of the audit the measures were simplified
and consolidated. One of the unexpected benefits of the audit was that it was clear that
customers had often not even noticed the signage in the stores. Our recommendation was
that the signage should be removed on a test basis in a number of stores to see if that made
any difference to the sales. The recommendation was accepted and tested in ten stores and
it was found that sales were not affected at all by the lack of signage. Therefore the signage
was cut back significantly from all stores, saving a huge amount of money. Despite the
earlier reservations by the marketing personnel we now became quite popular and we were
asked to carry out audits of many other key areas of the business.

Institute of Internal Auditors professional standards

The Institute of Internal Auditors as the official voice of the profession has been
championing the development of the activity for many years. The definition from the
Institute of Internal Auditors has been around for a couple of years.

Internal Auditing is an independent and objective assurance and consulting activity that is
guided by a philosophy of adding value to improve the operations of the organisation.

It assists an organisation in accomplishing its objectives by bringing a systematic and
disciplined approach to evaluate and improve the effectiveness of the organisation's risk
management, control, and governance processes.

A few of the key facets are highlighted below.

INDEPENDENCE

It is critical that Internal Audit is seen as an independent function. Internal Audit must not
have any other role and certainly no management responsibility. However, if independence
gets in the way of adding value, another of the key requirements as per the definition, there
is a dilemma. I firmly believe that the spirit of the definition relates to independence of
thought and relates therefore to objectivity, hence the reference to ‘objective assurance’.
Internal Audit must be shown not to be biased, not to be influenced emotionally or
politically by issues which come up in the audit. Adding value and objective independent
assurance are critical and complementary aspects of the risk-based audit approach.

CONSULTING

The topic which has generated a huge amount of discussion, the concept of the Internal Auditor
as a consultant might appear bizarre to some. To imagine the auditor as the oft-used joke,
someone who borrows your watch to tell you the time and then keeps the watch, would not be
a positive view of the role. However, having the wider remit and freedom that an external
consultant often enjoys could well be very useful. The main difference between consulting assignments and the other work is that I believe that consulting jobs must be requested. Such assignments will often be carried out in a completely different manner. It is now possible to carry out an Internal Audit by workshop. I have led a number of such ‘audits’ in my career. For example, if you are looking to audit a contract or a project or something with a start and an end, an excellent approach is to assemble the key personnel involved in the room at the same time and to ask them what are the things that have gone well to date, what hasn’t gone so well, what are the threats and areas of opportunity. You can then determine the areas you wish to test, complete them and get the same people back together and present your observations or report back to them and (hopefully) get some agreement to actions required. This is a very positive experience for management and what is more, they don’t even know they’ve had an audit. This is a very different type of approach and very much a consulting type of assignment.

ASSISTING IN ACCOMPLISHMENT OF BUSINESS OBJECTIVES

The next aspect of the Institute of Internal Auditors’ definition is that it assists an organisation in accomplishing its objectives. As risk-based audit directly relates to achievement of objectives, this is an entirely consistent aspiration. The words highlighted towards the end of the definition are that Internal Audit helps evaluate and improve the effectiveness of the organisation’s risk management, control and governance processes. Until recently this definition just referred to control – now risk management is referred to first. This again reflects the basis of a risk-based approach. The final key word in the definition is ‘governance’ and we will talk about this critical topic a little later. A second definition, one which you are probably not aware of, resulted from a piece of work done under the auspices of the Institute of Internal Auditors a few years ago to develop a competency framework for Internal Audit.

Internal Auditing is a process by which an organisation gains assurance that the risk exposures it faces are understood and managed appropriately in dynamically changing contexts.

The definition is very different and appears ‘light years’ away from the compliance orientation. This definition, whilst not formally adopted by the Institute of Internal Auditors, has been incorporated in part in their standards (2004 update). The wording is as follows:

Performance Standard 2600 Resolution of Management’s Acceptance of Risks

When the chief audit executive believes that senior management has accepted a level of residual risk that may be unacceptable to the organisation, the chief audit executive should discuss the matter with senior management. If the decision regarding residual risk is not resolved, the chief audit executive and senior management should report the matter to the board for resolution.

The implication is that Internal Audit should be looking at all the key areas of risk and how they are managed and, if Internal Audit believes the organisation has taken unnecessary risks or has risk exposures, which are unacceptable or too high, these should be discussed and agreed with management. As you will notice, the Institute of Internal Auditors standards state that, if there cannot be an agreement, this must be reported to the Board – a significant opportunity to influence at this level.
WHAT IS BEST PRACTICE?

Is it possible to define best practice Internal Audit? I am not sure you can do so easily. One way to explain best practice is that this is the process adopted by the most respected and successful functions.

We have developed a database of best practice based on information from over 3000 Internal Audit functions worldwide and when I refer to best practice in this book it will reflect the practices that the best follow and how they do so. One very clear message from such functions is to ‘forget the petty cash’, a euphemism, of course, not only for the petty cash but all minor issues, the issues that don’t really represent significant risks to your organisation. Someone could take the petty cash everyday and it wouldn’t really make a great deal of difference to your organisation, would it? It clearly does not mean that you should never audit these areas but make sure you keep such reviews in context and to a minimum.

RECOGNITION AND REPORTING LINES

Make sure that you are able to operate at the very highest levels in the organisation. If you are not having regular contact with senior management including the Chief Executive it is very difficult to know what the key issues are. A monthly meeting of the Head of Internal Audit with the Chief Executive is regarded as good practice plus a quarterly meeting (at least) with each of the other directors.

GETTING IN AT THE START

Internal Audit needs to be able to demonstrate its willingness to add value and work with management. An excellent way to do so is to offer to advise on key systems under development. It is much more valuable to identify areas of omission or controls needed at this stage. You will not be thanked if you identify these issues three months after the system has been implemented.

I have heard concerns expressed about Internal Audit being involved in systems development projects – the argument being that this might compromise independence – ‘how can we be involved in the project and then come in after implementation and audit the new system?’

I do not believe there should be any concern. Providing Internal Audit acts in an advisory capacity and is involved at key stages only and does not sign off the system then independence cannot be compromised. It is a critical aspect of the independence that Internal Audit should not be a signatory to systems, procedures or any other development. If they sign-off such activities then they are part of the process and their independence is inevitably compromised.

A further aspect of getting in at the start is to try to be ahead of events. If you can sit down with senior management and explain that you are planning an audit of a key topic and this happens to be the most important issue in his or her mind, you will be seen as proactive and the reputation of your function will be enhanced. Indeed the key issue in terms of risk-based audit is to look forward not back. You will get no credit for critiquing the past when management are facing the challenges of the future. Increasingly this will take you into ‘the crystal ball’ areas where there is little history and there isn’t a lot of
What is the role of the function? Policeman, risk assessor or consultant?

What is the role of the Internal Audit function in the modern era? Is it to police, is it as a risk assessor, or is it as a consultant? The general view here is that it has to be a combination of all three.

1. The role of police officer is not considered a very sexy image for the Internal Auditor but there has to be an element of policing in any Internal Audit role. The policing aspect is probably reducing but it must still feature in the role.

2. Risk assessor definitely features heavily in the modern audit role. An independent assessment of how well the organisation is managing its threats is clearly a very significant and important role.

3. Consulting, as we have seen earlier, is becoming a much more important aspect; indeed a completely separate set of guidelines are included in the Institute of Internal Auditors standards for professional practice. If you are trusted enough to complete a consulting assignment when the option is to engage an external consultant, then clearly that has to be an excellent vote of confidence. You have the capability to do a great deal within your Internal Audit role. Have confidence!!

How Internal Audit has developed

In considering the development of the Internal Audit profession, there are four distinct stages.

- **Stage 1 Traditional**
  The earliest and most traditional approach was a very detailed, often painstaking, audit focused almost exclusively on financial activities and which was totally compliance based and involved reviews of frighteningly large volumes of transactions. In fact, in some organisations, including banks, this type of audit was referred to as an inspection. Thankfully most Internal Audit functions have moved on from that very time-consuming approach. The biggest concern looking back was that in years gone by, Internal Audit were often part of the process (and not totally independent) because they were required, for example, to review and approve payments before they were made. This, happily, has been recognised as the management function it always was and passed over to them in almost all organisations. This convenient ‘crutch’ for management has now been despatched to the archives.

- **Stage 2 Systems Based**
  The next development within the Internal Audit function cycle was establishing a systems-based approach. Rather than focusing on individual locations, branches, and so on, you should audit the processes and systems looking across the organisation, a horizontal rather than vertical approach. The systems-based audit (SBA) approach
focuses on adequacy of controls rather than reviewing large numbers of transactions. SBA is recognised as much more constructive and collaborative.

- Stage 3 Developmental
  This is the modern approach to Internal Audit whereby you can and should audit any function in the organisation. A risk-based approach is adopted, focusing on the activities that really matter to the organisation, concentrating on the objectives rather than the controls and looking at the threats to their achievement. The emphasis is now on the overall business framework rather than individual systems with a view to identifying areas where accountability could be blurred, for example, where interfaces between functions occur. This is where most audit functions should be operating or at least should aspire to be.

- Stage 4 Forward Looking
  The final stage is to be even more forward looking:

  1. Looking for and getting requests, particularly for consulting-type assignments.
  2. Being regarded as a solutions facilitator rather than a function pointing out problems.
  3. Operating as a business partner, or maybe even an advisor and a mentor. This is the most positive role for Internal Audit and is the ultimate deliverable from the risk-based approach.

Summary

In summary, the essentials of risk-based auditing are widening the coverage, tackling some of the non-traditional areas and focusing to help management achieve their objectives. It requires a demonstration of greater knowledge of the business and, more importantly, allows a much broader level of assurance to be given to the Board. All these ideas are expanded in the subsequent chapters.