OPTIMISING ASSURANCE

Phil Griffiths

Managing Director

Business Risk Management Ltd

An examination of the corporate governance challenges to the various assurance providers in an organisation and how these functions can use the opportunity to optimise value added.

1. Introduction

More and more emphasis on governance, assurance and control is being espoused by recent regulation, standards and guidance, much of which is risk orientated.

How should the various assurance functions in a business rise to the challenge and how should the organisation manage such activities effectively and efficiently?

The Corporate Governance requirements now in place in most countries, looked at from a dispassionate viewpoint, could simply be regarded as a need for organisations to sign off the disciplines and processes already in place. However, the resultant debate and its intensity would suggest that companies are far from happy to do so.

The fulcrum of this debate is Risk Management. Most businesses believe they understand and can manage their significant risks, but the ever-growing list of well-publicised failures and problems indicate that such issues are not always fully understood.

As a result of the governance reforms, risk management has grown in just a few years from being a useful tool to become the very pulse of the organisation, and the way in which management of a company is judged.

No wonder tensions have been created. It should be no surprise that many Boards of Directors are uncomfortable in being asked to certify that they have reviewed the significant risks within their business – shareholders, after all, will be quite entitled to ask ' if all the significant risks have been reviewed (and presumably appropriate actions taken to mitigate them) why wasn't the recent disaster anticipated?'

This is a level of responsibility and open accountability that few directors will be comfortable. It also, of course, provides potential tension between the Executive and Non-executive directors- due to the recognition that the

Non-exec's role is now to monitor how well the organisation is managed.

It is clear, therefore, that the Board needs help, not just in reviewing the effectiveness of internal controls but also in providing assurance that all the significant risks have been reviewed. Furthermore assurance will also be required in ensuring that the risks are being fully managed and an embedded risk management process is in place.

This is a tall order. In many organisations this challenge is being passed to the Internal Audit function. The other assurance functions within the business are increasingly also being given responsibilities in this regard.

The challenge is not just for companies either. Government and other Public sector senior management is very aware that similar governance responsibility falls on their shoulders and are reacting accordingly. Corporate Governance is also likely to become a worldwide 'hot potato' very shortly as pressure to integrate the different corporate governance codes intensifies with the advent of the Sarbanes-Oxley Act in the USA.

So what does this all mean for the assurance providers?
Who provides the assurance?

2. The main Assurance functions

The UK Combined Code for Corporate Governance recognises that there may be a number of different assurance providers: -

' In conducting its annual assessment, the Board should consider the scope and quality of the ongoing monitoring of risks and internal control, and, where applicable the work of its internal audit function and other providers of assurance.'

2.1. Internal Audit

The internal audit role is covered in detail in section 3 but one look at the new Institute of Internal Auditors' definition of Internal audit shows clearly the risk and governance focus, which is expected.

IIA DEFINITION

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 organisations **risk management, control,** and **governance** processes.

The highlighted words assurance, risk management, control and governance provide a very clear direction for the function. The word consulting which has appeared for the first time is also significant, as it recognises the wider professional role required of the function in the governance and other arenas.

2.2 Compliance

Compliance is a function, which has been enjoyed particularly by organisations in the financial services sector, primarily due to the requirements of the legislation in this sector.

However the increasing regulatory environment elsewhere e.g. in the utility and telecommunications industries, together with new EU directives, the Data Protection Act and employment legislation to name but three have significantly increased the pressure on businesses to comply.

As the penalties for non-compliance can be extremely punitive – including the ultimate sanction, the loss of the licence to trade, the risks are considerable.

The compliance function is therefore of necessity risk-orientated but differs from Internal Audit in that unlike the latter function compliance cannot be totally independent (as the function also has non-audit duties). This is not in any way intended to denigrate the compliance function – indeed in some organisations the Heads of both departments report to the Audit Committee – but it does point to the need to co-ordinate the activities very carefully to avoid duplication and optimise added value.

Financial Services organisations have developed excellent templates for such co-operation and those can provide a good skeleton to help businesses in other sectors tackle the subject of regulatory compliance.

2.3. Health and Safety

Many organisations have dedicated functions to monitor and review the effectiveness of the Health and Safety disciplines within the organisation.

Failure of employers to provide:-

- **safe systems at work**
- **a safe place to work**

*** plant and machinery that is safe to use**
*** competent supervision and/or suitable training**
*** care in the selection of employees**

can again result in very significant fines and punitive action. Most organisations however tend not to evaluate health and safety in strictly risk terms, as one fatality, for example, is one too many. It is rare that Internal Audit, under their umbrella responsibilities passed down from the Board, review the effectiveness of the Health and Safety function or the risks associated with this topic. Encouraging these functions to work more closely together can only be beneficial to the organisation.

2.4. Security

Until a few years ago, in may organisations the security function has traditionally focussed on detection rather than prevention – understandable as many functions are led and staffed by ex-policemen.

However, a different approach is now being adopted, with security taking a much more proactive role. This is also tending to be risk focussed, although in many businesses I have seen, the Corporate Governance risk focus has not permeated down to the Security department. There is therefore a need for cooperation and education here – one which Internal Audit or Risk Management could take.

2.5. Risk Management

Many organisations have recognised the advantage of establishing a dedicated risk management function – reporting through a risk management committee to the Board. Many of these departments have evolved from an Insurance base to become broad-based with wide responsibilities. Typically the Risk Management function is responsible for ensuring that a comprehensive risk management programme is developed and implemented , and to ensure that the programme successfully enables the business to manage the many threats faced. In short it has responsibility for coordinating the risk management agenda.

It is therefore very important to ensure that all projects initiated within the business with a significant risk impact should be coordinated (if not owned by) this function in order that risk is managed under a wide-brimmed umbrella (and the organisation is not suddenly caught in a downpour , or worse a flood.)

Other assurance functions must develop a close liaison with Risk management to ensure efforts are harmonised. (This has been achieved In some organisations by a number of these providers now being managed directly by the Risk Management function)

2.6. Environmental Audit

A number of organisations with particular environmental sensitivities,

typically those in the chemical, nuclear and quarrying industries, together with those handling hazardous products, have established a separate environmental auditing function. These tend to audit against the environmental management system standard ISO 14000 and are of course risk focussed. However as recent well-publicised events in the nuclear industry have shown, the risks can be much greater than anticipated – in these cases fairly minor lapses have caused huge damage to the reputation of the businesses. Businesses in other sectors should therefore take heed. Environmental risks are likely to be significant for most organisations within the next few years (if they are not already). For organisations without an environmental audit capability, serious consideration should be given to buying in the expertise ,this should help encourage the business to take the risks seriously, notably those posed by pollution and waste management.

2.7. Quality Assurance

Many organisations have established Quality Audit teams to review all processes and activities covered by their quality systems, under the International Standard ISO 9000 (and its derivatives ISO 9001, 9002 etc.)

The role tends to be carried out by internal quality auditors who complete the audits on a part-time basis, either being employees of the organisation with other responsibilities or external personnel subcontracted to carry out the work.

These reviews are by necessity compliance oriented as the objective is to assess the extent of conformance with the quality procedures, but they are becoming more risk orientated as the functions and processes embraced by the total quality approach expands.

The standards for internal quality auditing are also becoming more stringent. The next version of ISO 9000 (expected in late summer 2000) will require that internal quality auditors have sufficient recent experience and have formal auditing qualifications,(all of which is incorporated in a soon to be mandatory Auditing Standard ISO 10011)

A real opportunity is therefore offered to refocus the activities of the Quality audit team towards areas of significant risk, to assist in the Corporate Governance evaluation process. It also provides the opportunity for a much closer relationship with the Internal Audit function and the Risk Management team

2.8. Insurance

Many risk management committees were originally established and led by the Insurance Manager – as a vehicle to build awareness of insurable risks and to help the organisation to introduce programmes and specific actions to reduce losses and claims.

Whilst this was, and is, a laudable objective, most organisations have recognised that the majority of significant risks in a business are not

insurable.

To their credit it tends to be the Insurance functions that have been leading the crusade to consider the wider risk agenda.

Opinions vary as to the proportions of insurable to uninsurable risk but a generally accepted model is that of the iceberg:-

Just as only 1/10th of an iceberg is visible above the sea so typically only 1 in 10 of significant risks in a business are insurable.

It is therefore crucial that the Insurance function is brought fully into the risk assurance process, and that they have significant knowledge of the variety of risks impacting the business. In this way they can add substantially to the Corporate Governance process.

2.9. The Audit Committee

The expectations and responsibilities of Audit Committees are becoming ever wider and, of course, now encompass risk. As recently as 2002 little mention of risk was made in may audit committee terms of reference.
A survey of 155 companies carried out at that time revealed the roles of the audit committee to be as follows:-

	% of Companies
Selection of external auditors	78%
Assessing the system of internal control	74%
Reviewing the scope and approach and results of external audit work	62%
Accounting/reporting policies and procedures	51%
Reviewing the results of Internal Audit work	31%
Agreeing the internal audit plan	31%
Agreeing audit fees	29%

Since then the key focus has very definitely changed to include:-
Ensuring the company has effective processes for identifying and managing key business risks.

It is, therefore, the Audit Committee in many organisations that is taking the reins as far as the risk aspect of the Corporate Governance agenda – hence the logical and powerful role for Internal Audit in this regard. (as IA is normally the only function with a direct reporting line into this body)

It is, therefore, crucial for the Head of Internal Audit to build a very strong relationship with the Chairman of the Audit Committee, specifically to:-
* **recognise the audit committee as their client;**
* **understand the committee's expectation and respond accordingly;**
* **communicate with and meet regularly with the Chairman.**

*** communicate with the committee with candour and openness.**

2.10 External (Statutory) Audit

External audit are also very much linked in with the whole corporate governance agenda given the reporting requirements that they have under the Combined Code. As a result ,the external auditors are increasingly being asked to communicate qualitative judgements about accounting principles ,disclosures and risk. By doing so, the external auditors can add to the effectiveness of the board of directors in monitoring corporate performance and risk management on behalf of the shareholders and in assuring that shareholders receive relevant and reliable financial information.

It follows therefore that a close relationship between the External and Internal auditors (and to a lesser extent the other assurance functions) should exist.

In many organisations it is my experience that the external auditors have been unable to gain sufficient reliance from the internal audit function due to the fact that the Internal audit programme was not focussed at a high enough level. Focussing the internal audit activities towards the most significant risks provides an opportunity to get this reliance.

Internal audit should therefore take every opportunity to develop a close working relationship with their external auditors as much mutual benefit will accrue.

3. Assurance at the crossroads

Having worked in Internal Audit for 20 years and had close involvement with the other assurance providers, I have seen the roles change from verification and low-level checking to ones which in many organisations have carved out reputations for driving change and business improvement. The assurance providers , however, probably face the greatest challenge (and potential rewards) in their history.

This provides a potential "shot in the arm" for the function, particularly as the provision does highlight the advantages of having an adequately resourced and professional I A function.

Nonetheless the "kill-rate" for in-house internal audit functions is increasing in the UK, following a significant trend in the US. The Big 5 firms of accountants and other specialists have, quite correctly, identified opportunities to provide high quality, competitively priced internal audit services on either an out-sourced or partnering basis.

I do not intend to discuss the arguments for and against outsourcing or partnering but suffice it to say the Big 4 would not be providing the service unless they regarded it as a function that was important and would add value.

Exactly the same arguments apply to other assurance providers, particularly Quality Assurance, Environmental Audit and Insurance.

The challenges are those provided by the Combined Code, and the business risk agenda in particular.

3.1 So is Business Risk a lifeline or noose for Assurance providers?

Whether in-house or externally provided, the focus of the assurance functions in the first decade of the 21st Century has to be risk.

Audit Committees and Boards need the assurance functions to help them evaluate the effectiveness and efficiency of their systems of business risk management.

This should ensure that the functions have a high profile, particularly if the business risk focus is communicated widely within the organisation (which it should be). NB for those functions, which have not specifically marketed themselves by means of a brochure, web pages, intranet pages, newsletters etc. – this is an ideal opportunity to do so.

The high profile created and the necessity to give a considered opinion to the Board and the Audit Committee on the significant business risks and how effective they are being managed, could also have negative connotations.

If the assurance providers have reported to the effect that the business risk management processes are effective and major problems or surprises subsequently occur, this could significantly impact on their credibility.

There is also a further dimension. In may organisations, one of the assurance functions have been asked to lead the Business Risk Management programme or elements thereof. I.e. establishing and leading workshops, collating the results etc.

Under these circumstances it could be argued that their independence has been compromised. Who then will review the effectiveness of the process?

The key, I believe, is to co-ordinate the activities closely with the other assurance functions and, of course, management, to establish a clear agenda and the role and responsibilities of each function. This is further discussed in the conclusion (Section 6).

In this way, Corporate Governance and Business Risk in particular should be the vehicle for the assurance departments to develop a more influential and significant role than has been possible before. But for many departments this will involve an enormous amount of work and a change in culture.

3.2 What needs to be done?

To be able to rise to the significant challenges faced, the biggest issue cited was to enhance the skills within the function,

The IIA having also recognised this fact commissioned a very significant research project which culminated in the publishing of the 'Competency Framework for Internal Auditing'

The authors, William Birkett, Mona Barbera, Barry Leithhead, Marian Lower and Peter Roebuck are all highly experienced professionals and the resultant framework offers an extensive and highly relevant template for developing internal auditors.

3.3 The Competency Framework (CFIA)

The framework examines the challenges faced by the modern internal auditor and provides a structured set of roles and competencies, based on three elements of the internal auditors lifecycle – the new joiner (described as the entering internal auditor), one with 2 or 3 years experience (the competent internal auditor) and internal audit management.

The elements of the key business processes form the basis of the framework. These are translated into units.

The Competency framework fully recognises the importance of risk and assurance as the following extracts show

Unit 1. Develop understanding within the organisation about the risks associated with its functioning and contexts.

1.1 Understand an organisation's objectives/strategies, process capabilities and contextual dynamics.
1.2 Profile the organisation's attitude/stance on risk.
1.3 Understand the risk management strategies of the organisation.
1.4 Provide advice/recommendations relating to the organisation's risk management philosophies and strategies and their implementation.

Unit 3. Contribute to improvements in the functioning of the organisation's risk management and control systems.

Unit 4. Provide ongoing assurance to the organisation that it is "in control" relative to its risks.

4.1 Establish Assurance strategies/plans

4.2 Establish the scope of assurance projects

4.3 Identify/develop the methodologies relevant to an assurance project

4.4 Establish a project plan

4.5 Conduct the assurance work

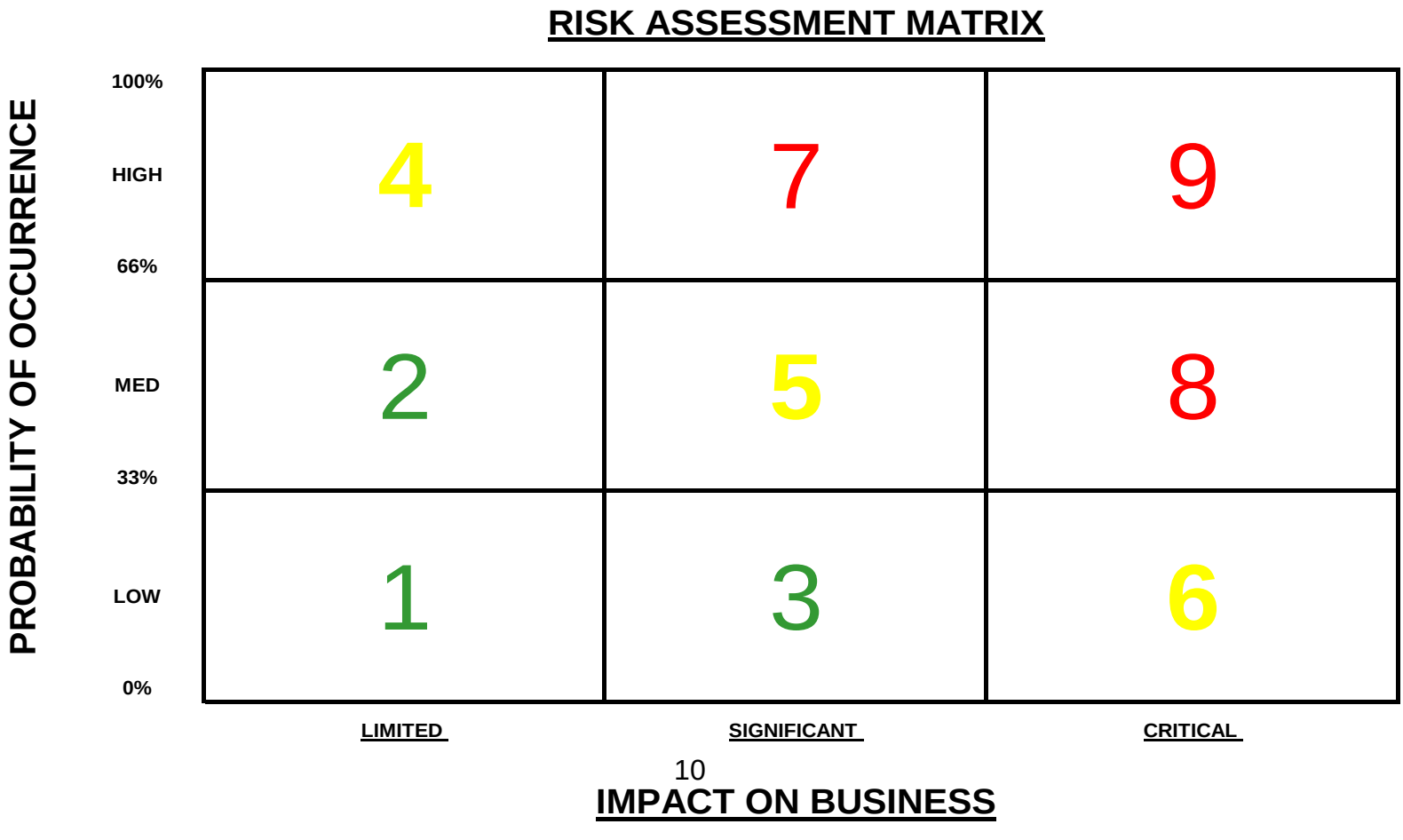
4.6 Communicate the results with relevant parties

Any assurance function embracing the framework embodied within CFIA will not just achieve best practice, but be in a position to build long-term credibility and trust.

It will also significantly aid their aspirations to play a key role in the full assurance agenda.

4. Monitoring and reporting of significant risks.

Control Self Assurance provides a vehicle for management to establish a through and properly managed business risk programme, and also the means for "self-audit".
It will however be the assurance functions (and primarily internal audit) that will review the effectiveness of the programme and to monitor the very risks and report to Senior Management.
The Business Risk programme will identify the key risks faced by the organisation and their relative significance, normally plotted on a Boston box matrix (as below)
The internal audit function should ensure that the risks at the top right of the matrix (those in boxes 7-9 at least) are directly translated into the basis of their programme. My experience is that these risks should form the



basis of at least 60% of the total audit programme.

In this way IA are being seen by the business as proactive and focussed – it is much easier to "sell" the benefits of an audit if the topic is recognised as critical to the success of the organisation.

Other assurance functions should also be fully aware of the matrix and plan their activities accordingly.

4.1 Perceived versus actual controls

Management will have given their evaluation of the effectiveness of the actions, procedures and systems in place to mitigate the significant risks identified during the risk workshops, and, probably again, in control self assessment questionnaires. Internal audit and other assurance functions will then, as part of their on-going audits, need to assess the accuracy of these perceptions and, of course, the effectiveness of the controls in place.

Reporting on the results of the audits (notably the accuracy of the perceived mitigation and ,of course, needs to be handled sensitively. This is discussed further in the paragraph on audit reporting.

Another important task often given to assurance providers in relation to the Business Risk programme is to review the actions achieved against those planned – to ensure that exposures are treated effectively and in the required timescale.

4.2 The need for multi-level reporting

Direct involvement of the Internal audit and other assurance functions in the business risk and corporate governance arenas provides the opportunity to enhance the profile and recognition of the functions, but only if the reporting process is managed effectively.

The Assurance functions have the opportunity to report on a number of levels – each one requiring a different approach.

To functional management

Reports to functional management on the perceived versus actual controls to mitigate key risks should focus on the opportunity to enhance control rather than a "you said …….. we found" approach. Specific benefits and business opportunities should be highlighted wherever possible. Actions must be agreed to tackle additional exposures before Board reporting.

To the Board

A quarterly summary of the results of the audits should be presented giving a picture of the overall accuracy of management's evaluations (in my experience, this having been generally sound) and an exception based schedule of the impact on risk exposures – especially further or more

significant exposures identified – together with the actions agreed to tackle them.

A quarterly progress report on the action plans to address the risk exposures identified in the business risk programme should also be presented.

To the Audit Committee

The Audit Committee report (at least 3 times a year) should focus on achievement: -

*** What actions have been implemented;**
*** the benefits achieved (monetarily if possible);**
*** the extent to which the risks have been reduced (using the Boston box matrix is a very good idea);**

*** What competitive opportunities have been identified/exploited;**
*** the % accuracy of perceived versus actual mitigation;**
*** the percentage coverage of the most significant risks achieved by Internal audit.**

4.3 The need to coordinate reporting activities

Each assurance function within the organisation will have its normal reporting hierarchy – normally via the Executive with responsibility for the activity.

It is important to ensure that the messages received by the Board, the Audit Committee and Risk Management Committee are consistent and accurate.

To do so requires coordination. This can be achieved in a number of ways. One way is for a nominated function (e.g. Risk Management or Internal Audit) to receive reports from the other assurance functions on their activities, and for the Head of this function to extract the risk implications for onward reporting.

Another method is to have each function prepare a monthly or quarterly report, specifically relating to risks covered and the key findings. These reports can then be put together into a pack (with a summary) for onward transmission to the Board etc
This method has the advantage of enhancing ownership.

A third approach is to circulate individual reports widely between the assurance functions and ask the heads of the departments to compare and contrast the findings with their own – enabling reports for their Executives to be more balanced.

I favour a fully coordinated approach with one function taking

responsibility for extracting the key issues (with accompanying reports from each assurance function)

5. Conclusions

The governance and business risk challenges posed by the combined Code provide considerable opportunities for the assurance functions in a business to demonstrate their important contributions. A much more coordinated approach is, however, necessary if this is to be truly successful.

The following is a suggested model or paradigm:-

Current Approach	Required Approach
Assurance functions roles and responsibilities less than clearly defined.	**Very clear terms of reference for each function defined and approved by the Audit Committee – to ensure no overlap (misunderstanding).**
Assurance functions have separate reporting lines and are not coordinated.	**Reassess reporting lines – ensuring all report to a Board Director. Establish a clear written method of coordination – responsibility being given to one of the assurance functions.** **Heads of functions should meet together quarterly** **Share annual plans** **Agree not to visit same location in the same quarter** **Determine optimum function to review each area**
Assurance functions have different objectives and not all formally consider the implications of risk.	**Ensure objectives of each function embrace risk and clearly identify the roles and responsibilities in relation to risk reporting.**
Internal Audit may not base its programme on the most significant risks in the business.	**Internal Audit must ensure that at least 50% of its programme is directly based on the most significant risks identified by management**.
Role of Internal Audit and other	**Audit Committee and Board to agree**

assurance functions in the business risk process often poorly defined.	**specific role of Internal Audit and other assurance functions in the development of the business risk programme**.
Assurance functions are afraid of getting too involved in CSA or risk workshops lest their independence is compromised.	**Get as involved as possible (as this will add the greatest value). Define the boundaries carefully and recognise that the role is not 'audit'. Independence will therefore be unaffected.**
Mix of skill in many assurance functions is limited.	**Develop skills and competencies using the CFIA framework as the basis.**
Many assurance functions are not properly represented on the "top table". As a result their contribution is not valued as it should be.	**The Business Risk and Governance agenda provides a significant opportunity. All functions must therefore demonstrate what they can do – and therefore earn the recognition they deserve.**
Assurance functions are often accused of not working together with management.	**Coordinating activities and leading CSA activities will build much closer relationships and enhance trust.**
Many reports produced by assurance functions are lack-lustre and fail to promote change.	**Refocusing reports on risk and making them much more positive will transform the value delivered by the functions.** **At least once a year provide a joint report to the Audit Committee or Board– with input from all assurance functions**

Ever increasing shareholder expectations and the need to achieve demanding growth, profit , safety ,environmental and other regulatory targets pushes organisations into taking bigger and greater risks.

To survive in this environment , an effective risk management and control framework is essential. As a result independent , positive assurance that such frameworks are effective and efficient is vital.

Professionally focussed assurance activities provide organisations with this assurance.

Risk and opportunity go hand in hand and assurance functions, if properly coordinated, can also provide organisations with advice and guidance on the relationship and balance between risk and control.- enabling you to make the right decisions.

Phil Griffiths