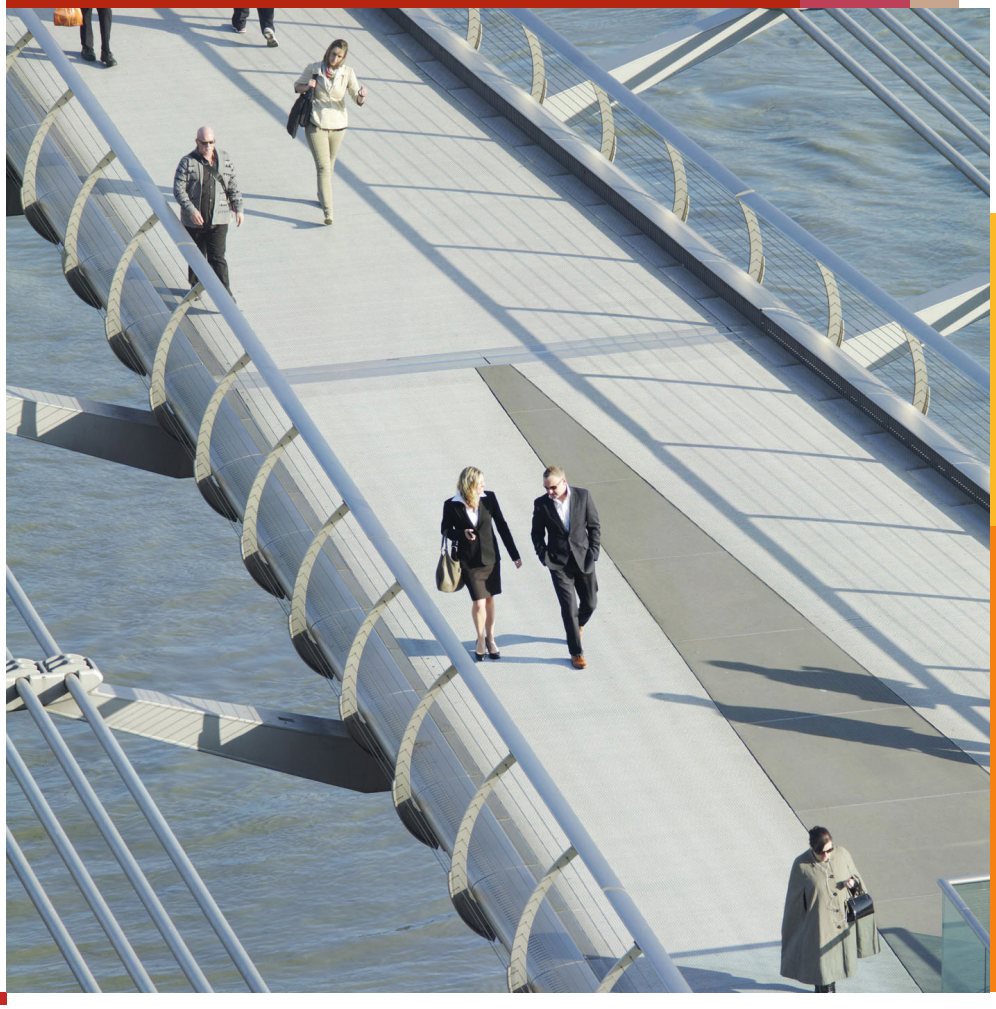
Governance of Risk

Written by Rob Newsome, Director of PwC

12 June 2011



pwc

Contents

Why the current focus on risk?	*1*
"Black Swans"	*3*
Risks vs. Risk Events	*4*
Risk Measurement	*5*
Risk Appetite	*8*
Risk management maturity/effectiveness	*11*
Loss events and remediation	*15*
Risk software	*16*
Role of the CRO	*18*
Risk assurance	*20*
Risk and Audit Committees	*24*
Risk Reporting	*26*
Key Risk Indicators	*27*

Why the current focus on risk?

Risk sound bites.....

Risk management is being acknowledged as an increasingly important discipline. These sound bites are aimed at providing the reader with succinct insight into some of the key issues impacting on risk management and governance.

Recent events have highlighted the need to move risk management up on the importance scale for Boards and executive management.

These events include the Icelandic volcano, the Gulf oil spill, Japan's tsunami and the Sishen mining rights. In the financial services industry, the continuing focus on risk through Basel II and III for banks and Solvency II (in SA Solvency Adequacy Management [SAM]) for insurance companies has created more regulatory pressure on ensuring the adequacy of risk management.

The global credit crunch has also destroyed the myth that business will continue as it always has and now business needs to be far more able to respond and react to changing conditions. Risk management is seen as one of the key disciplines needed to prosper and survive in the world economy today. Note that many commentators have attributed poor risk management as one of the causes of the credit crunch.

'Black Swans'

The high impact low probability events are called 'Black Swans'. [In Europe, as legend has it, they only knew swans as white so black swans were not possible].

'Black Swans' are the events that wipe millions off the market capitalisation of corporations such as BP and Arcelor Mittal. CEOs and boards now want to know what potential Black Swans the corporations they are responsible for managing could face.

This has opened the debate about the quantification of risk. These events now need to be included in the risk considerations. Typically, risk management quantification identified only those risks that management considered not sufficiently managed.

The Black Swans typically can't be prevented but the responses to the consequences are significant. The approach being followed now is in considering events that will have specific consequences – e.g. collapse of distribution channels, loss of key suppliers, sudden significant exchange rate changes etc. The risk event becomes less important as the recent history has shown that these can be off the radar!

Risks vs. Risk Events

Solvency II and ISO 31000 have focussed on the identification of risks. In Solvency II the capital that needs to be allocated to risk has to establish what risk or risk event needs to be considered. A general risk of, say, loss of skills cannot be measured. Similarly, 'underground fire' in a mine is not sufficiently articulated to establish the possible extent of the event – it could be at the stopes, or on moveable machinery, or in the shaft etc.

Risk events need to be distinguished from the higher level risk names in order for the risk to be managed. 'Competition risk', for example, cannot be managed as a generic matter.

The risk event will be a new market entrant in a region, specific product substitution, or product pricing; these potential or actual events can be managed. Similarly 'loss of skills"' needs to be unpacked to the events that have to be managed, such as what to do when the aging engineers retire and no obvious replacements have been identified.

All risks that are evaluated as having a potentially substantial impact on the organisation/business should be unpacked to constituent risk events.

Risk Measurement

Risk measurement is an art and not a science. There are certain risks that the actuaries will model to come up with a very scientific assessment of the possible risk exposure. There are others that achieve a high, medium or low assessment [green, yellow or red, for us boring accountants].

The key elements that should be included in the measurement are as follows:

- There should be sufficient differentiation to allow a meaningful priority rating to be achieved. This can be on a 100 basis points scale, on a monetary scale, on a numeric scale.
- The current risk position should be established, taking into consideration the current risk mitigation/controls. This is known as the residual risk.
- The risk exposure before control or maximum possible loss should be evaluated to determine the extent that existing mitigation/ control is managing the risk; this is often referred to as inherent risk.
- The amount of risk that the organisation is willing to accept should also be determined; this is known as risk tolerance or desired residual risk.
- The residual risk gap should be determined to establish the extent that remediation is required and to prioritise this remediation.

Below is an example of applying the measurement scales:

- Impact scale on 100 basis points.
- Inherent likelihood on a percentage scale.
- Control effectiveness on a percentage scale.

Impact		100
Likelihood		60%
Inherent Risk	Impact x Likelihood	60
Control Effectiveness		40%
Residual Risk	Inherent Risk x Control Effectiveness	36
Desired Control Effectiveness		80%
Risk Tolerance	Inherent Risk x Control Effectiveness	12
Residual Risk Gap	Residual Risk - Risk Tolerance	24

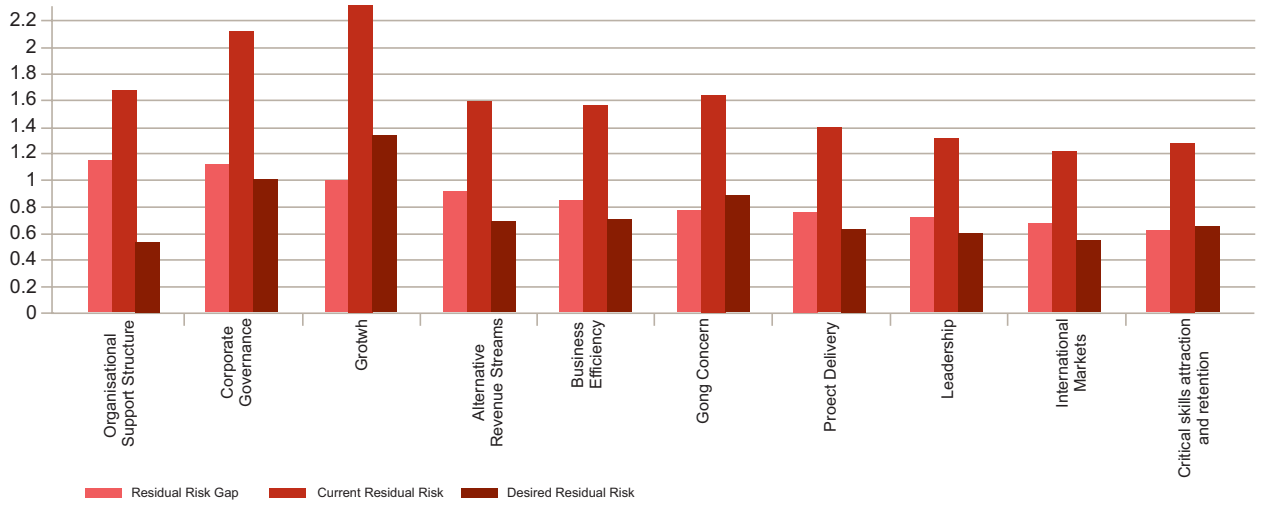
Other developments in measurement include

- Frequency of the risk exposure is receiving more attention now to understand the risk better. For example, the risks associated with plant operations are a daily exposure, while contract risk is on an as and when basis.
- Risk controllability is the extent that the risk can be managed or mitigated. For example no organisation can control the Icelandic volcano that disrupted air travel to Europe – which in turn had a major impact on fresh fruit exports. The only mitigation then is to manage the consequence.
- Using Monte Carlo simulations to assess more scientifically the potential and residual exposures – often used for contingency funding assessments on projects. There are many other quantitative models that are used.

The graph below demonstrates the results of applying the measurement concepts discussed above. The residual risk gap provides the priority for addressing the risk exposures.

Strategic Risk Assessment

Bar Graph: Top 10 Residual Risk Gap



The results provide a basis for understanding the risk exposures without having to get a precise measurement.

Solvency II and Basel II have put the focus on measuring the incidence of risk and the extent that capital has to be matched against identified risk. Interestingly, Basel II requires reserves to be kept based on the experience of residual risk without considering the other measurement criteria set out above.

Risk Appetite

Risk appetite is the most misunderstood concept in risk management. How much risk is an organisation willing to accept? Or does the organisation have an appetite for risk? How does this tie back to performance management?

Risk appetite and tolerance are often misunderstood and are therefore often not applied in practice. Financial Services (FS) have a better practical feel for the concepts with the value at risk and how much value can be risked – in total and per product/investment type. Non-FS companies have a more difficult time in making the concepts realistic.

Below is an example of a typical risk appetite statement.

Key elements	Peer example risk appetite statements
Capital	• Maintain an insurance insolvency ratio of at least 150%. • Maintain a ratio of insurance risk economic capital to life insurance reserves below 10% at all times. • Maintain a ratio of credit risk economic capital to total bank lending book exposure below 4% at all times. • Hold as a minimum sufficient economic capital to withstand a one in 200 loss on a one year basis • On an economic basis, we week to maintain an AFR/Ecap ratio of at least 100%. • Hold sufficient capital to maintain the group's published core financial strength ratings in the AA rating range.
Earnings	• Our earnings will not fall below budget by more than 10% more frequently than once every 5 years. • No expected loss to a single customer within the loan portfolio will be greater than 10bps of our own funds. • Achieve steady, sustainable growth in operating profits o an EEV and IFRS basis. • No one exposure to a single financial institution counterparty, other than intercompany exposures, will be greater than 5% of Group Available Financial Resources and exposure will only be to counterparties recognised in the relevant policy (e.g. above A+ for derivatives).
Liquidity/ALM	• Positive cashflows in extreme but plausible stress scenarios. • No appetite for financing required cash-flows in a manner detrimental to its main external stakeholder. • General Insurance liabilities are matched as closely as possible with assets of appropriate amount, type (fixed or real) and currency.
Reputation	• Our people will have the highest levels of competence and integrity. • We will treat our customers fairly. • We seek to continue to have top quartile customer satisfaction in all of our core markets.
Other	• We target an S&P rating of A+ on our senior debt. • We seek to fully meet all regulatory expectations. • We will have no tolerance for international regulatory breaches.

These high level statements provide parameters for risk consideration and intersect with strategic objectives and corporate value statements.

The above risk appetite statement describes the parameters of strategic positioning as well as providing clarity on strategic intent. But it does not easily reach to the actual risks that need to be addressed. Some organisations are looking to the underlying risks.

Other appetite statements include, for example, a statement that risk appetite is described as an event that will impact 5% on EBITDA and will result in a 10% change in market capitalisation (share price). Potential risks are unpacked to risk event level and evaluated to provide a most likely value. This value is compared with the appetite.

We have taken a view that risks should be measured on their potential impact on the achievement of strategic objectives.

Risk levels		Risk decisions		
Risk Category	Inherent Risk	Current Residual Risk	Risk Appetite	Risk Exposure above Rrisk Appetite
Compliance	17%	19%	13%	6%
Financial	33%	28%	14%	15%
People	19%	22%	15%	7%
Product	7%	15%	10%	5%
Strategic	3%	30%	30%	0%
Systems	22%	33%	15%	18%

Legend

- Risk Exposure Above Risk Appetite: Less than 30%
- Risk Exposure Above Risk Appetite: Greater than 30% but less than 60%
- Risk Exposure Above Risk Appetite: Greater than 60%

The inherent risk for each strategic objective is assessed for the risks allocated to the strategic objective. The current residual risks for all risks per objective are aggregated to be expressed as a percentage and this is compared with a similar value achieved for risk tolerances, which in aggregation is termed as 'Appetite'. The difference highlights the extent that the current position is outside of appetite. Ultimately, it identifies the risks exposures that need to be managed to achieve strategic objectives.

A similar view per executive risk owner provides another interesting oversight.

The real buy-in happens when the appetite is expressed per risk owner - the C Suite for enterprise wide risks!!

Risk management maturity/effectiveness

Standards and Poors (S&P) is the first rating agency to publish its criteria for assessing the effectiveness of risk management that they include in their credit and investment ratings. This direct linking of availability, duration and cost of funds to risk management has elevated the focus on risk management effectiveness.

Many organisations are now assessing the effectiveness or maturity of their risk management processes. This allows benchmarking and focus on specific areas for improvement.

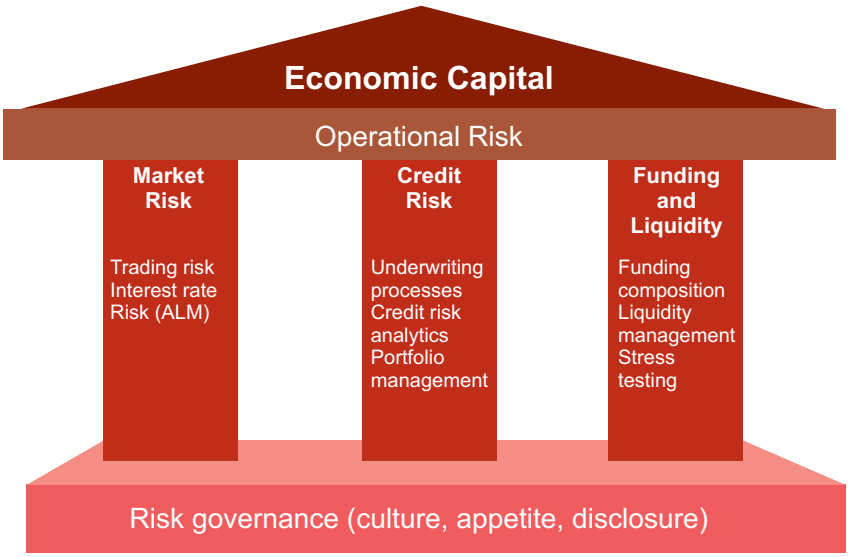
Implications

S&Ps four-level scoring scale provides a public gauge as to a company's risk management capabilities and practices.

Weak	• Firm has limited capabilities to consistently identify, measure, and comprehensively manage risk exposures and thus, limit losses. • Sporadic execution of its risk-management program.
Adequate	• Manage risk in separate silos, but maintains complete control processes. • Firm loss-/risk-tolerance guidelines less developed, but risk and risk management often considered.
Strong	• Demonstrates an enterprise-wide view of risks, but still focused on loss control. • Risk and risk management usually important considerations in the firm's corporate judgement.
Excellent	• Demonstrates risk/reward optimisation. • Well-developed capabilities to consistently identify, measure and manage risk exposure and losses.

How is Risk Management structured?

ERM Evaluation components for financial institutions



The base on the Parthenon provides the framework on the actual management or risk. The assessment of the effectiveness of risk management for the 'pillars' or 'rafter' is a fundamental assessment of management effectiveness.

The assessment of the base is where the focus of Risk Management effectiveness/maturity is positioned.

Typically, the following elements are assessed.

- Organisation and Governance
- Strategic Planning and Risk Appetite
- Risk Policies and Standards
- Risk Identification and Representation
- Risk Measurement and Reporting
- Risk Communication and Escalation
- Infrastructure
- Stakeholder Disclosure

An assessment can produce the following result.

ERM Element	Basic	Developing	Developed	Advanced
Organisation and Governance		(1) 1	(2) [4] 2	(2) [1] 2
Strategic Planning and Risk Appetite		(3) 2	[1]	1
Risk Policies and Standards		(2)	[2]	2
Risk Identification and Representation		(1) [1]	(2) [2] 3	
Risk Measurement and Reporting		(3) [3] 3	(1) [1] 1	
Risk Communication and Escalation		(6) [3] 3	[2] 2	1
Infrastructure	[1]	(3) [1] 1	[1] 1	1
Stakeholder Disclosure		(2)	[2] 2	
TOTAL	**[1]**	**(21) [8] 10**	**(5) [15] 11**	**(2) [1] 7**

(UK) [SA] PwC

This is based on the details as set out below.

#	Key ERM element	Criteria	Illustrative Practices	Maturity level			
				Basic	Developing	Developed	Advanced
1	**Organisation & Governance**	Robust Board/senior management direction and oversight	The structures and policies have recently been introduced and established.	The governance structures do not identify the Enterprise Risk Management Framework.	An Enterprise Risk Management Framework has been prepared that defines the risk policy and procedures but does not fully establish roles and responsibilities.	The Enterprise Risk Management Framework clearly defines key roles and responsibilities.	The ERM framework provides the structure and purpose of the risk management activities and its continual relevance is assessed at least on an annual basis.
2		Coherent Board and management committee structures to facilitate effective reporting and oversight	The Audit and Risk Committee has recently been constituted and an Audit and Risk Committee has been combined.	Audit and Risk committees have not been specifically established to consider risk. Risks are considered to be addressed through the performance review structures only.	Audit and Risk committees have been established. Mandates are not clearly established and there is substantial overlap of risk consideration at the various committees.	Audit and Risk committees have been established with approved mandates and reporting requirements. Formal reporting to the committees takes place with some overlap of risk considerations.	The board committees set risk strategy, approve limits and policy, oversee risk profiles and validate risk appetite on a periodic basis. The management committees integrate all aspects of risks, including risk specific committees that address market, credit, operational and compliance risks. They review the enterprise risk profile, evaluate key risk drivers, approve detailed policies and escalate key relevant issues to the Board. The effectiveness of the committees is reviewed annually.

#	Key ERM element	Criteria	Illustrative Practices	Maturity level			
				Basic	Developing	Developed	Advanced
3		Centralised risk function led by a Chief Risk Officer (CRO) with credibility, stature and clear reporting relationship with CEO	The CRO position has been recently established and an appointment made. The CRO is supported by a department that oversees the assurance activities and the operational and bank risk functions.	No CRO is appointed. Risk management activities are completed by Compliance or Internal Audit.	The CRO function is incorporated into line managers' responsibilities –.	A dedicated CRO is appointed with reporting through to Chief Actuary or equivalent. The CRO has effective interaction with Corporate Group Risk Management.	The CRO is appointed at a senior management level with direct reporting to the CEO and he/ she attends/ is represented on Exco. The risk management function has adequate resources (people, support tools, etc.).
4		Clear definition and allocation of company-wide roles and responsibilities	The CRO position has been recently established and an appointment made. The CRO is supported by a department that oversees the assurance activities and the operational and bank risk functions. The risk management responsibilities in the bank have not been fully implemented.	Risk management responsibilities are not specifically identified. Reliance is placed on the performance management and specialist risk processes (such as actuarial modelling, etc.) to manage risk exposures.	Risk management processes are established to consider market, credit, operational and fiduciary risks.	Risk management is clearly defined as a line management responsibility. A specialist risk function (such as actuarial modelling, etc.) provides input to the business unit for risk management considerations. Internal audit reviews the effectiveness of the ERM processes. Business units have allocated risk champions.	Risk and control owners are established with specific responsibility to ensure that the risk/ control information is accurate and frequently assessed and remedial action is completed. Accountability for risk is reflected in incentives and rewards.

These assessments are typically reported to the Board through the Audit or Risk Committees.

Loss events and remediation

- Loss events occur throughout the business/operations throughout the year.
- There are many audits/reviewed conducted throughout the business that identify potential loss events.
- Self assessments and planning events also identify areas of business that need improvement.

All of the above inform on the effectiveness of the management of risk. The events etc should be linked to the risk exposures to determine if the underlying risks have been identified or if the current risk evaluation is accurate.

The challenge is to capture the events, near misses, improvement opportunities and to link them to the risks.

Some organisations have processes and systems to record loss events, usually through the health and safety efforts. Basel II enforces the recording of events for banks. Usually there are diverse practices in recording the events and improvement opportunities and there is no attempt to link these to risk and to provide a centralised record of the events and improvement opportunities.

Following on from the loss events and improvement opportunities is the remediation effort required to address the loss event and improvement area.

A centralised approach where risks are linked to risks will provide effective remediation consideration, as priorities can be established. The tracking of remediation is then enabled and can be reported to management and governance levels. Targets can be set to address a priority percentage of identified remediation.

Such an approach prevents a shopping list of actions that keep getting carried forward year on year.

Risk software

What software should an organisation adopt? The default is a plethora of spreadsheets!

Risk software should assist in embedding risk management and enabling management to easily execute its responsibility and to access and report on the risk data. The software should be able to migrate into other applications such as compliance, control self assessment, and assurance coordination.

The selection of the most appropriate software should consider the following matters:

- Reputation of the vendor and financial position of the vendor to be able to continue in the market and support the applications. This can be determined through market share, shareholder support, international exposure, existence of user groups etc.
- The extent of development work and capacity for such work that the vendor is undertaking. The vendor should be refining the software to improve its functionality based on user experiences and requirements, as well as taking into account risk management trends and developments.

- The flexibility of the software solution to support related risk activities such as control self assessment, compliance risk management, assurance mapping and results, incident/loss event tracking, and remediation control.

- The software should have a flexible reporting capability that is easy to apply to the risk data. Risk data should easily be able to be turned into business knowledge. The report writer functionality allows the user to slice and dice the risk information to provide the relevant information at the touch of a button. The report writing may depend on the degree of user configuration allowed vs. the use of standard methodologies that create the reporting fields.

- The extent of user configuration will determine the level of customisation that can be achieved without vendor support. This is important to allow for customisation without becoming too dependent on the vendor.

- The software should be accessible though normal communication protocols established for remote connections.

- The software should not require any specialised hardware or supporting software to function.

The software should allow for easy data update and reporting by the users to minimise the time spent on ERM administration. Risk processes that require extensive management/ user attention to maintain the data will most likely result in management fatigue with risk management in its entirety.

Generally our advice is to not develop in-house solutions. These systems are not core to the organisation and will most likely not be properly maintained as they will be of low priority for the programme maintenance people, and there will be few programmers who will know the system as it will not be worked on by many. We have seen systems developed by a couple of individuals that fall over quickly when these individuals move on or lose interest.

Banks and other complex financial service organisations will have sophisticated risk management systems, as risk is a core to their business and to meeting stringent regulatory requirements. Basel II has seen banks invest significantly in risk management solutions and Solvency II (Solvency Assessment and Management – SAM – in South Africa) may see a similar investment by insurance companies.

Role of the CRO

Chief Risk Officers (CROs) are now an established position in many organisations. In financial service organisations the position is often at the executive level, given the significance of the different risk exposures and need for specialists to manage these risks.

In other organisations, in both the public and private sectors, the role of the CRO is not that clear. Non financial institutions have only recently considered risk management as a separately constituted management discipline.

Often, risk management grew out of the internal audit function as they were at the initial stages and well versed in the risk management concepts, as they had been applying them for years in their audit work. This was a practical development for many organisations. Internal auditors are part of the governance fabric and can apply the requirements to demonstrate, to their Boards and Audit Committees, that the organisation is in compliance with the requirements/ recommendations of the PFMA, the Combined Code and King etc.

The merging of risk management and internal audit is not an ideal or lasting solution. Risk management is a management process and must be owned by management. Internal audit should be in a position to review the adequacy of such a process and should therefore be independent of its functioning.

The CRO should have sufficient organisational status to enable him/her to be effective. This can be achieved through the reporting relationship to an executive member and governance committee of the board.

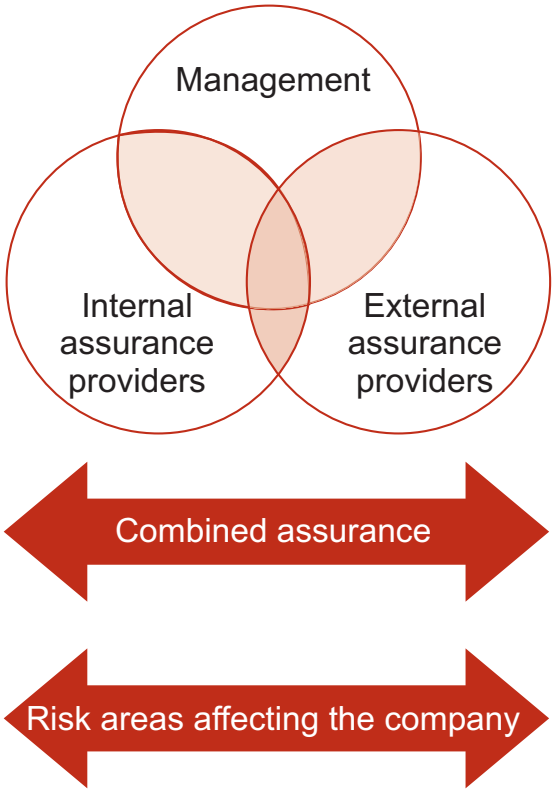
The CRO is responsible for facilitating the risk management process. Line management is responsible and accountable for ensuring that the risks are effectively managed. The CRO should facilitate the risk management processes. These include –

- ensuring that the risk management policy and framework are appropriate for the organisation and include leading practices as appropriate and achieve regulatory and governance compliance;
- ensuring the risk assessment processes are properly and timeously completed;
- coordinating and preparing the risk reporting to the executive and board committees;
- facilitating bench marking of risk exposures and risk mitigation measures as appropriate;
- assisting with the coordination of the combined assurance/ risk assurance activities;
- preparing the annual risk management plan;
- reporting on the extent that the plan has been achieved;
- providing challenge to the risk exposures identified by management;
- liaison with regulatory authorities when necessary;
- facilitating the integration of related risk activities into the risk management process such as compliance, IT governance and environmental;
- the management of the risk management software or platforms;
- monitoring and reporting on the recording of loss events and risk remediation;
- testing the risk evaluation against actual experiences inclusive of loss events;
- providing ongoing risk training to management and the board;
- executing the risk management communication strategy;
- ensuring risk is included in management agendas and is fully considered during strategy development; and
- liaising with insurers and the facilitation of the insurance cover renewals.

Risk assurance

Risk assurance is best achieved through the combined assurance approach recommended by King III.

Combined assurance model



[1]

Combined assurance should be based on identified risks and how assurance is achieved and reported to the board through the audit committee. It offers tangible benefits that extend well beyond proving compliance, including:

- Coordinated and relevant assurance efforts focussing on key risk exposures;
- Minimised business/operational disruptions;
- Comprehensive and prioritised tracking of remedial action on identified improvement opportunities/weaknesses;
- Improved reporting to the board and committees, including reducing the repetition of reports being reviewed by the different committees; and
- Possible reduced assurance costs.
- The use of combined assurance to support the audit committee and board in making their control statements in the integrated report.

A 5 step approach to establishing combined assurance is set out below:

1. Establishing the business case
2. Assurance reality check
3. Risk mapping
4. Combined assurance design
5. Making combined assurance a continuing reality

[1] Ibid.

1. *Establishing the business case*

Who are the assurance providers and what assurance do they provide? Create the assurance universe and map the assurance accordingly:

Strategic goal	1st layer of defence		2nd layer of defence			3rd layer of defence			
	Control self assessment	Management review	Risk management	SOX	Compliance	Internal audit	External audit	Quality	Special project
Financial									
Treasury									
HR									Culture climate survey
SCM									
Product & services									
Customers									Customer feed back

Gaps and over auditing are often identified.

2. *Assurance reality check*

The assurance that is provided should be credible. The generally unknown assurance providers are often where the focus needs to given. Key matters for consideration when assessing the credibility of the assurance are set out below:

- Independence and objectivity;
- Skill and experience;
- Qualifications;
- Assurance methodology; and
- Accreditation/affiliation.

Assurance is provided through the three lines of defence.

First line of defence	Second line of defence	Third line of defence
Management oversight	**Management of risk**	**Independent asurance**
Nature of assurance: Line management is accountable and responsible for the management of risk and performance. A key element of this activity is the extent of management revies and the actions that follow. Managmenet can establish a system of self assessments/audits to inform them on the adequacy of risk management activities.	**Nature of assurance:** Corporate functions provide support to line management in executing their duties. These include functions such as HR, procurement, compliance, risk management, quality assurance, Health and Safety, sOX, Tax, Engineering, Forensic (Fraud Risk Management), OEMs, Insurance, Actuaries.	**Nature of assurance:** Internal audit, Certifications, Regulator reviews, External Audit, Technical Audit, Forensic Investigations, external asset management reviews (e.g. Matrix) valuators, culture climate surveys, assessment of ore/mineral reserves (SRK)
Reporting Lines: Executive Managmeent Committees and Operational Committees providing direction, guidance and oversight over the focus the areas.	**Reporting Lines:** Risk Committees, Compliance Committee, Audit Comittees, Regulatory Forums, HR Forums, Health and Safety briefings.	**Reporting Lines:** Regulators, Board and Audit Committees, (objectivity is a key criteria), C Suite.
Assurance provided: Management as evidenced through the management review meetins and forums. Reporting on the results of self assessments/CSAs. Special projects that assess the operating effectiveness. Efficiencies – these can be internally or externally sourced. The assurance is reported to line management SWOT.	**Assurance provided:** Report to Risk Committees, Audit Committees, Health and Safety committees, Sustainability Committee, management meetings, Reports to regulators and external agencies (e.g. HACEP), ISO Certifications, equiment status reports. Risk management profiles.	**Assurance provided:** Reports to Board Committees, management meetings, insurers, regulators.

3. Risk mapping

Assurance is provided at the risk level. The existing assurance should be mapped to the risk profiles. This step will require the most effort to establish an effective combined assurance approach and is likely to take a relatively long time to complete. This detail is vital to ensure that combined assurance delivers its potential value to the organisation. It will also set the foundation for consideration of other assurance efforts that may be introduced in the future.

Risks can be defined at a strategic level to detailed process areas. Some assurance cannot be assigned at a process level (e.g. government relations), while others cannot be assigned at the strategic level (e.g. fall of ground at a mine).

In the analysis, the different lines of defence will be mapped to the identified risks in terms of work actually performed and the assurance expected.

4. Combined assurance design

The key output from step 4 is the blueprint for combined assurance – The Assurance Map.

What assurance is to be provided to whom?

This step identifies the recommended area of assurance and needs to articulate the nature of the assurance activities:

Example: Biannual mine visits by independent consulting engineers to verify progress against mine plan. The assurance will be reported to Exco, who will report to the board on the assessment completed. This may also be included in the integrated report (annual report).

Agreeing on a common universe

The risk profile must be established in a manner that is relevant to the business/operations and is managed on a consistent basis. Risk information is often maintained independently in the different business/operational units or by the assurance providers.

The integrated risk management approach recommended by King III should provide the foundation for the establishment of the assurance universe, thereby providing a sound base for establishing the assurance footprint.

Acceptable methodology/credibility

Assurance provided must be credible. This is achieved by ensuring that the skill and experience levels of the assurance providers are appropriate for the work to be performed, and that the extent of the work performed will address the potential and actual exposures.

5. Making combined assurance a continuing reality

A combined assurance champion must be identified to implement the approach. There should also be an executive sponsor who is able to provide the required authority for the project.

Internal Audit or Risk Management is usually best placed to take on the combined assurance champion role. They have an overall understanding of the business, are familiar with the assurance concepts and have a strong vested interest in making sure the approach is effective.

The diligence and effort in establishing an effective combined assurance approach must be matched by ongoing efforts to ensure the approach provides the value it is designed to provide.

King III requires internal audit to provide assessments of internal control (including internal financial controls) to the audit committee. Given the diversity of risks and controls required, internal audit cannot realistically provide this assessment without considering and relying on the combined assurance approach. Internal audit could provide its assessment of internal control by reporting on the adequacy of assurance provided by the implementation of combined assurance. Internal audit will need to assess the continued adequacy of the design of the combined assurance blueprint as well as how well the assurance has been provided.

Risk and Audit Committees

King III recommends that risk and audit committees be established. The Companies Act makes the audit committee a statutory requirement. Many companies and organisations are considering how risk committee and audit committees should co-exist or combine.

Audit committees have traditionally considered the appropriateness of the financial reporting and the findings of internal and external audit. King III has added oversight of the Integrated Report and combined assurance to the audit committee responsibilities.

The risk committee is a relatively new addition to the corporate governance scene. Many organisations are only now considering the appropriateness of such a committee. The agenda of these committees is accordingly fluid – there is no generally accepted minimum matter to consider.

The biggest areas of overlap between the audit and risk committees lie in the consideration of risk.

Audit committees were introduced to risk through the consideration of internal audit coverage. This is going to be further piqued through overseeing of combined assurance.

Risk committees are considering how risk is identified, evaluated and monitored. In the financial services industry there are different risk committees – some executive and others being part of the governance structure – such as Alco and Credit Risk. In non-financial services sectors the risk agenda is quite fluid.

Executives and directors often complain about the same issues being considered at numerous meetings/agendas of the board committees and at the board. This overlap is acutely felt at the risk and audit committees. This is often the impetus that creates a merged audit and risk committee.

We believe the following should be the basis of consideration between the audit and risk committee function:

Audit Committee	Risk Committee
• Oversight and approval of Integrated Report	• Ensuring effective risk management approach is implemented and in place
• Appointment of external auditors	• Approval of the annual risk management plan
• Consideration of external audit results	• Approve risk disclosures in the Integrated Report
• Oversight of the effectiveness of the internal audit function	• Consideration of appropriateness of the risk profiles and management ownership of risks
• Consideration of the internal audit findings	• Review of incident/remediation management
• Approval of combined assurance approach	• Consider reports on the status or risk and risk management
• Consideration of the actual assurance provided per the combined assurance activities	
• Consideration of results of combined assurance and findings where appropriate	

The risk committee needs to be careful in considering performance vs risk management. Many of the matters that are key performance matters that are considered at board level are also key risk management issues. So the risk committee should not become a quasi-board in debating performance matters.

The company secretary should ensure overlap of board and committee agendas are addressed. For example, sustainability related risks may be considered at a Sustainability Committee and should not be discussed at the Risk Committee.

Audit and risk committees are often combined due to the members of the committees being substantially the same, or the agenda accommodating both areas of responsibility.

The danger of the combined committee is that risk gets relegated to as and when there is time to cover the required matters. The relegation is understandable given the Audit Committee statutory status and the number of years it has been established.

Organisations will need to consider the need to split the committees based on complexity of the business/ operations and the ability of a combined committee having sufficient time to effectively cover both the risk and audit committee matters.

Risk Reporting

The top ten risks are the most common reports presented to Risk Committees or equivalent. They are compared to prior periods with appropriate commentary.

This is in sufficient to provide a proper picture of the management of risk and risk management. For example, how does the risk committee know that risk 15 should not be included in the top ten?

The risk management reporting should include:

- the status of the risk plan;
- risk identification/evaluation activities completed;
- to provide a view of the currency of the risk profiles;
- any scenario sessions held and results;
- the status of the remediation for identified risk exposures (through loss events, audit findings, self assessment); and
- any audit report on the maturity/effectiveness of the risk management activities (this should be assessed at least bi-annually).

The management of risk reporting should include:

- assessed risk exposure to appetite;
- aggregated risk exposures and changes from prior periods per strategic objective;
- significant cross-cutting risks across the operations and the respective exposures; and
- top evaluated risks – biggest movers from prior periods, actions needed to reduce big exposures, reasons why risks are rated so highly.

Key Risk Indicators

Key risk indicators (KRIs) and key risk management indicators are often used interchangeably. KRIs measure the risk impact on the business whereas key risk management indicators are used to measure the effectiveness of the risk management process. This sound bite addresses the KRIs.

A KRI is an indicator of the possibility of an adverse impact or upside potential. KRIs provide an early warning to identify potential event(s) that may impact the ability or disability to achieve set objectives. KRIs can be quantitative or semi-quantitative.

A KRI is a measure used by management to indicate an activity's level of risk. It differs from a Key Performance Indicator (KPI) in that the monitored risk is specifically known and tracked; while the KPI is a more general measure of business performance.

Typically KRIs:

- track the trend or status of a risk over a period of time based on quantified underlying information;
- provide a perspective on the performance of controls;
- generate insights; and
- improve decision-making.

Our experience is that organisations KPIs and KRIs are used interchangeably. A KPI may be a hurdle rate or value to achieve. A KPI measures the risks in play – very often these are reported within the organisation as a matter of course but not recognised as such. For example, the collections from debtors provide risk information about the recoverability of the debt and the need to assess existing controls. Risk profiles should be linked to the KRIs to understand the underlying risks and remedies when the KRI indicates attention is needed. The profile should provide a direct link to the KRI. Sometimes targets are set for each KRI. These targets reflect risk tolerance.

The KRIs need to be determined considering conceptual significance, ease of implementing and maintenance, etc. Grading and warning criteria for individual KRIs need to be specified. Examples provide a practical insight to understanding their essence.

Risk Type	Value Driver	Area	Analysis By	Risk Indicator
Operational Risk	Expense	People	Employee Category	Trend in HR claims, e.g. disputes, employee injuries, casualties, etc.
				Change indicators
				Complexity Indicators
				Complacency Indicators
			HR Indicators	Loss from Labor disruption and inflexibility (% work force unionized % overtime)
				Impact of termination rate, absence rates, turn-over of key strategic talent and head-count
				Impact of Employee Index, Mobility rate and training investment rate per Employee

Risk Type	CSF/Value Driver	Area	Analysis By	Risk Indicator
Business Risk	Revenue	Sale Effectiveness	Call Centre	Volatility of channel Revenue
				Volatility of Win/Loss Ratio
		Product Mix	Existing Products	Product Revenue Volatility
			New Products	Volatility of X Revenue as a % of Total Revenue
				Revenue Volatility
				Volatility of M&A Revenue
		Customers	Channel & Segment	Revenue vilatility attributable to Customer index changes
				Volatility of Customer Chum Rate
Market Risk	Revenue	Currency	Exposure Type	Sensitivity of foreign exchange exposure
	Expense	Interest Rate		Sensitivity of floating exchange exposure
		Equity		Sensitivity of equity exposure in Employee stock option plan and Venture capital investments
		Employee benefits		Sensitivity of Employee Benefit Plan
Regulatory Risk	Revenue	Regulatory Evironment Change	Segment	Revenue/EBITDA Impact from Regulatory proceedings
	Expense	Compliance		Losses derived from frequency and severity of Compliance penalties