The Role of the Risk Professional in Leading the G in GRC

Governance, risk and compliance disciplines are converging – risk professionals will need to continue to broaden their skills to maximise career opportunities

RMIA
RISK Management Institution of Australasia

The Risk Management Institution of Australasia Limited (RMIA)

About RMIA

The Risk Management Institution of Australasia Limited (RMIA) is the largest professional association and peak body for risk management in the Asia-Pacific region. Members of RMIA cover every sector of the economy and all levels of government. RMIA's members are located predominantly in Australasia and there is a growing membership internationally.

The RMIA is a leader in professional education, providing recognition of core competencies, the provision of top class networking events and in driving thought leadership in the management of risk and realisation of opportunities. RMIA provides two accreditation designations for its members, including Certified Practising Risk Manager (CPRM) and Certified Risk Management Technician (CRMT).

Through its active participation in policy setting forums and the publishing of standards related to the risk management profession, the RMIA keeps members and other interested parties abreast of key industry developments as well as helping to ensure risk management guidance to organisations is pertinent and adds value.

Authors

Bryan Whitefield – Director, RMIA Chapter Operations

Judy Clarey – Director, RMIA Education & Professional Development

About CPRMs and CRMTs

The CPRM (Certified Practising Risk Manager) and CRMT (Certified Risk Management Technician) designations are RMIA accreditations designed to provide confidence that our risk professionals have high levels of expertise and competency. These peer reviewed licences represent the highest levels of practice at two important stages of a Risk Manager's professional career. CPRM and CRMT members have demonstrated significant skills and knowledge gained through experience, qualification and a commitment to ongoing professional development.

Acknowledgements

The RMIA would like to thank the members of the CPRM Masterclass of 2012 for sharing their knowledge and experience which will aid their fellow colleagues in the risk profession; the editorial sub-group of CPRMs for their editorial review and input to the paper; Bryan Whitefield, Director of Risk Management Partners and Director, RMIA Chapter Operations, for his efforts in facilitating the Masterclass and Judy Clarey Director, RMIA Education & Professional Development Committee as convenor of the CPRM Masterclass.

About the paper

Early in 2012 RMIA's Education and Professional Development Committee conducted a survey of CPRMs to understand their key areas of interest for the GRC Conference Masterclass. From the feedback received, "the role or future of risk in the GRC debate" was clearly flagged as an area of interest by respondents. This led to the development of this Masterclass session topic by Bryan Whitefield in consultation with other CPRMs.

The paper provides a commentary of the key GRC concepts presented by Bryan as discussed by participants on the day.

Risk professionals will need to lead on certain elements of governance to ensure risk takes an appropriate place in the business.

Background

Many governance, risk and compliance (GRC) professionals would agree that much of the past decade has been spent discussing what GRC is and isn't, its current business drivers and organisational benefits as well as the common barriers or blockers currently being experienced by many organisations.

As risk professionals we have a good understanding of where "risk" fits within a GRC framework, but for many of us the ongoing challenge will be: how to "lead" key stakeholders across the organisation to the same understanding? In order to do this, risk professionals will need to lead on certain elements of governance to ensure risk takes an appropriate place in the business and its control framework.

We will also need to overcome our own personal biases and those of others in the organisation tasked with establishing and operating an appropriate GRC framework. As the GRC industry has converged we have seen the influences of the various professions from which many risk professionals have come including accounting, audit, engineering, legal, project management and safety. Each profession brings with it a view of the world that is centred around its core strengths and, as risk professionals, we know that our aim is not to manage a particular set of risks, or manage risks in a particular way, it is to help ensure an organisation is aware of and competently managing risk across the full breadth and depth of the business. A very tough assignment in most cases.

On the face of it, it would seem that as a risk professional you need to understand strategy, finance, safety, project and change management, organisational behaviour as well as have a great understanding of the business you're in. On top of that, you need to show strong leadership across all of them! In fact you better be someone with an MBA on steroids.

Herein lies the opportunity for risk professionals. No matter the profession you are from, an effective GRC framework will require both generalist and specialist knowledge. As risk professionals, we have developed much of this knowledge already. This discussion paper explores what we already know and what we may need to learn to enhance our opportunity to lead our organisations down the GRC path in an ever evolving business world.

Risk Professional: For the purpose of this discussion paper the generic term of "risk professional" refers to the diverse range of titles given to those with responsibility for the oversight and management of an organisation's risk portfolio – which includes the frameworks and systems for risk profiling and reporting.

You need to understand strategy, finance, safety, project and change management, organisational behaviour as well as having a great understanding of the business you're in. On top of that, you need to show strong leadership across all of them!

The Masterclass

The Masterclass was provided an introduction that outlined:

- The converging worlds of governance, risk and compliance.
- The growing need for GRC to be integrated as businesses become more complex, stakeholders increase their expectations, regulators are given more powers and society remains litigious.
- The roadblocks for risk professionals are almost identical for the broader GRC profession including:
    - Perceptions of GRC as a wet blanket or a handbrake on business
    - Time/resource pressures on staff across organisations
    - A tendency for the designers of frameworks to make them more complex than they need to be
- The primary imperative of GRC is the same as for risk management – outstanding performance across the business.

Following on from the introduction - workshop participants were invited to put forward their ideas on the role of risk management in the GRC debate and more importantly the role of the risk professional in a GRC Management Framework.

Participants worked in groups to review a selection of reference readings that related to the four discussion topics outlined in Table 1. Each group discussed and shared their ideas and experiences on their specific topic with a view to providing feedback and recommendations to the rest of the group.

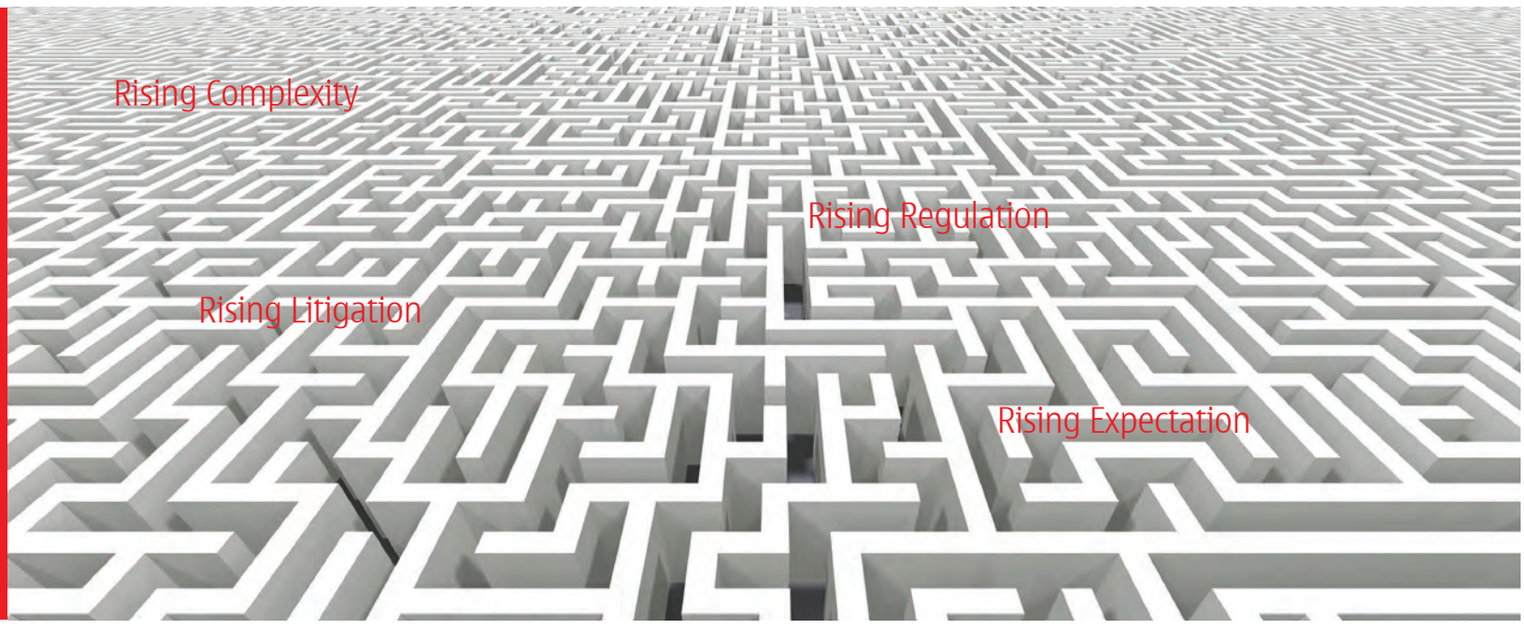

Table 1 - Group Discussion topics	
Group Discussion Topics	References
1. Which came first, the chicken or the egg? What are the implications for the role of the Risk Professional in leading the G in GRC?	Governance and Risk; “Risk Governance” Models; By EY and Deloitte
2. What is/should be on the minds of Boards? What are the implications for the role of the Risk Professional in leading the G in GRC?	Board Surveys: PWC Directors Survey/AIRMIC Directors Guide/AIM Governance Survey
3. What do the survey and whitepaper tell us about the GRC landscape, in particular the R in GRC. What are the implications for the role of the Risk Professional in leading the G in GRC?	The GRC Landscape: OCEG GRC Maturity Survey by KPMG-ICAA GRC Paper
4. What is the role of a G professional in GRC? What does it take to move there from the R in GRC?	Defining the Ultimate GRC Professional: Evolving Role of Governance Professional; CECO/CSA

As expected, with so much experience in the room, the debate was vigorous and new themes soon arose.

Key Challenges

Although the discussion and debate around each of the discussion topics was as diverse and extensive as expected given the background and experience of group members, a range of underlying but inter-connected issues and challenges were identified.

Table 2: Key Challenges	
What GRC is and isn't	It was clearly acknowledged during group discussions that GRC means different things to different people and that often the real challenge for risk professionals is that each individual term – governance, risk, and compliance – can have varied meanings across an organisation. Creating a common understanding across an organisation was seen as a first imperative.
What are the implications for the role of the risk professional in leading the "G' in GRC?	A growing regulatory environment, higher business complexity and increased focus on transparency and accountability have led enterprises to pursue a broad range of governance, risk and compliance initiatives. However, these initiatives are sometimes uncoordinated in an era where risks and their controls need to be interdependent. As a result, these initiatives get planned and managed in silos, which potentially increases the overall business risk for the organisation. In addition, parallel compliance and risk initiatives lead to duplication of efforts and cause costs to escalate. This highlights the need for the G in GRC to be well managed and hence creates an opportunity for risk professionals.
What capabilities and attributes do risk professionals need to lead and influence within a GRC environment?	The strong links between an organisation's strategy, business performance, and culture were a central topic of conversation by all groups throughout the day. There was consensus on the notion that high-performing companies view culture as an enabler of strategy and performance, and strive to create a culture that will support corporate governance and business sustainability. Given this – the question arose, exactly what does the risk professional's "super hero" suit look like?

What GRC is and isn't

There were many views on what GRC is and is not. In fact there was significant debate as to whether GRC was in fact an appropriate term for what it is evolving into. One perception was that integrated GRC is nothing more than enterprise risk management (ERM) repackaged by solution providers to drive a new market while others countered that ERM was a distinct subset of GRC.

GRC is

Many saw GRC as a federation of business roles and processes – the corporate secretary, legal, risk, audit, compliance, IT, ethics, finance, and other business streams – working collaboratively in a common framework and architecture to achieve agility, effectiveness, and efficiency across the organisation.

GRC for many workshop participants is seen simply as an approach to business - a business approach that should permeate organisational values, oversight, culture, business objectives, management functions, disciplines, processes, and boundaries.

Without doubt, workshop participants understood that an effective GRC program should focus on determining the right strategies and objectives for an organisation to pursue, then provide assurance that these strategies are executed and objectives achieved.

It was acknowledged that GRC has become a widely accepted terminology for a management framework that provides boards and stakeholders with "assurance" that the organisation is being well managed now and is well set for the future. Some of the key elements for a sound GRC framework articulated by the groups are shown below.

Clearly communicates the Organisations / Boards vision and values across the business - to internal and external stakeholders

Supports organisational culture and behaviours that lead to a greater understanding of organisational objectives and increased productivity

Is "holistically" governed and managed via "performance based" accountability and responsibility structures

Establishes processes to manage risk within boundaries of risk appetite and tolerance set by the Board

Sets transparent and measurable KPIs for business outcomes, legal/regulatory compliance obligations, social responsibility and sustainability commitments

Creates a code of ethics, policies, and procedures which are clearly understood by employees, business partners and the wider community

Maximises the effectiveness and efficiency of governance, risk and compliance functions by ensuring appropriate interrelationships.

"When it (a strong GRC framework) is working well, you have created a self-sustaining system – sort of a self-licking ice cream!"
CPRM Masterclass Participant

GRC is not

From the discussions and debate across all the groups there were those who clearly acknowledged that GRC is not:

- Another label for enterprise risk management (ERM), although GRC can encompass ERM;
- Reliant on a single individual or governance, risk, or compliance functions;
- About silos of corporate governance, risk, compliance operating independently of each other;
- Focused on only reporting "upwards";
- About providing the Board/ Key Stakeholders with just "good news";
- Based solely around technology solutions– though technology can play a critical role.

What are the implications for the role of the risk professional in leading the "G' in GRC?

With increased scrutiny from shareholders and regulatory bodies, corporate boards and executive teams are more focused on "governance" related issues than ever before. The governance process within an organisation generally includes reporting and evaluation of business performance via strategy scorecards, risk scorecards and operational dashboards. Ideally, the "strategic" governance process integrates all these elements into a coherent process to drive corporate performance.

Group discussions confirmed that alignment and convergence of risk initiatives with governance and compliance functions is underway in many organisations.

There were those who proposed that the real challenge for the risk professional in these organisations was to "lead" rather than be "led" by governance and compliance activities while on the other hand there were those that thought the challenge for the risk professional was more about being in a position to "strongly influence and inform" the governance process.

However both camps agreed that establishing and maintaining "credibility at Board and C- suite level" was for many risk professional the biggest challenge to overcome. A challenge often compounded by the fact that:

Boards and Senior Management

When boards and senior management turn to their organisations' risk information for insight, they are often unimpressed by what they see. Many organisations - non-finance industry companies in particular - are still in the early days of fully integrating risk information with business information leaving their top management and boards with scarce or poorly structured information on the key/material risks facing the company.

In addition, many of these companies have a proliferation of processes that collect information on risk (e.g., complex risk registers; workshops; environment, health, and safety scorecards; project risk assessments) that together give risk management a bureaucratic reputation, often with justification.

Division and Line Management

In spite of Board endorsement , middle management in particular often view risk management processes as a burden rather than as good managerial practices.

Many business managers across the organisation "rule the roost" and resist having risk managers challenge the assumptions that underscore their business planning, strategy and performance reporting processes. Consequently the risk management function in these organisations is often seen as a "handbrake" rather than an "accelerator" of strategic thinking and governance.

> Credibility and trust must be earned and can only be achieved when the input from the "risk professional" is directly attributable to "value created"

Some Tried and Tested Strategies

a) Building Credibility

Becoming a trusted advisor is not achieved overnight. CPRMs, CRMTs and other Masterclass participants had many views on how to build towards trusted advisor status. Here is a selection:

- Risk professionals add real value to the strategic decision making process when they are able to assist others to understand the uncertainties around potential impacts or the assumptions underlying the decision.
- For many a key step in enhancing credibility is often accomplished by identifying opportunities to reduce complexity and hence the cost and effort expended on managing significant risks.
- The most successful risk transformations are usually led from the top - so it follows that clarifying through the organisation's risk charter the ultimate responsibility for oversight of the organisation's risk policy and appetite rests with the Board and it should clarify the responsibilities of the full Board and its committees.
- An effective way to jumpstart risk thinking at Board level is to create a risk "dashboard" that truly fits the needs of top management. An effective risk dashboard is an extension of the reports and documentation that top management already use
- To enhance credibility the risk management framework and system across the organisation must have its own house in order.

b) Getting the House in Order

The mention of the need for risk advisors within organisations to have their own house in order sparked plenty of further discussion and another series of views on what this means and how it can be achieved. Here is a selection of the views given:

- Resist using a "one size fits all" approach as each management area within a GRC management framework needs to be tailored to the needs of the organisation.
- Risk profiling and reporting within a GRC framework should allow the organisation to "assess once and satisfy many".
- Having a unified "risk management" framework and system should allow organisations to:
  - Take a consistent and harmonized approach to risk management.
  - Develop a common "organisation specific" language for risk activities throughout the organisation;
  - Set standards to help reduce duplication of effort across business lines;
  - Have the option to utilise an integrated GRC technology solution to manage repetitive activities and to streamline reporting.

People within the organisation are often the primary barrier to effecting change.

c) Taking Action

With the house in order, risk professionals are well set to provide the valuable advice good managers seek. There are many ways managers seek this advice and many ways risk professionals seek out opportunities to provide it. Again, here is a selection of views from the Masterclass participants:

- To ensure that risk management activities are aligned with governance requirements, the risk professional should establish and maintain ongoing communication, collaboration and coordination initiatives across the key functional and business groups in an organisation.
- In relation to improved collaboration between key stakeholders, functional areas and business units, the risk professional could take a lead role in a "triage approach" to problem solving – where decisions, issues and conflicts (like patients in emergency situations) are sorted and prioritised.
- As an agent of change the risk professional must understand the culture of the organisation and in particular the culture and behavioural norms of the key stakeholders involved in the governance processes. People within the organisation are often the primary barrier to effecting change.
- To influence culture and lead change processes, the risk professional must understand the business and its objectives. In particular the key business management systems and processes central to effective governance. Understanding the structure and process hierarchies for each major division of the organisation will help identify critical overlaps, interrelationships and areas where integrated GRC activities can be improved to enhance performance outcomes
- Demonstrating the "value add" of risk management in the governance process will be "evolutionary, not revolutionary". An organisation's governance, risk and compliance requirements and methods will change over time and governance practices will evolve with greater emphasis on integrating risk and compliance functions.
- It goes without saying that an ongoing role of the risk professional will be to facilitate the identification, engagement and training of risk functional process owners to ensure that critical processes are continuously maintained and improved. Having an end to end view of these key processes will help the risk professional understand and manage risks between divisions.
- Last but not least is the risk professional's role in providing strategic and operational business management information in a timely, accurate and accessible manner to support "informed decision making" and ultimately good governance. There is an increasing reliance on technology solutions designed to deliver risk information "data". These technology solutions need to be customised to reporting requirements of the business, and must have the capability of being able to respond quickly to changes in the business environment.

At the operational level, GRC based software solutions should be easy to use for varied and infrequent users, present relevant data to the user, ensure consistency across processes, and empower users. Minimal requirements could include configurable workflow routing, business and project monitoring, and interactive communication capability. Central to an effective system are document management functions capable of notifying the "right people at the right time" about the status of risk and compliance activities.

What capabilities and attributes do risk professionals need to lead and influence within a GRC environment?

There was absolute consensus that high level leadership and management capabilities for risk professionals are essential and that they go hand in hand. Though it was acknowledged that they are not the same thing, they are inextricably linked, and complementary.

There was discussion around the differences between management and leadership with "management" described as being mostly about "structure, systems and processes" and "leadership" mostly about "people and behaviour".

Listed below are some of the other differences discussed, many of which have been previously acknowledged by leadership and management gurus such as Warren Bennis, Peter Drucker and others

- The manager's job is to plan, organize and coordinate; the leader's job is to inspire and motivate.
- The manager relies on control; the leader relies on trust.
- The manager has a short-range view; the leader has a long-range perspective.
- The manager asks how and when; the leader asks what and why.
- The manager always has an eye on the bottom line; the leader's eye is on the horizon.
- The manager accepts the status quo; the leader challenges it. (Adapted from Bennis 1989)

For a risk professional it is important that leadership is not dependent on an in-depth knowledge or understanding of a particular issue, management function, its methods and processes. Leadership primarily depends on two key attributes or capabilities – possession of a range of attitudinal qualities (for example integrity, courage, compassion) and a sound understanding of human behaviour.

> "Leadership is not dependent on an in-depth knowledge or understanding of a particular issue, management function, its methods and processes"

When a risk professional understands this, they are more accepting of leadership portrayed by those in the organisation without a strong background in risk, who nevertheless understand the core principles and believe in them. Identifying strong allies is an opportunity not to be missed.

Other leadership issues discussed included:

- Leadership is something that can be learnt. Leadership is a matter of personal conviction and believing strongly in a cause or aim, whatever it is.
- The impact of generational characteristics on one's preference and/or tolerance of leadership and management styles was discussed, along with the differences between "Baby Boomers" and "X", "Y" and "I" generations. It was acknowledged that although leadership responsibility sometimes comes to people later in life, age is no real obstacle.
- Leadership can be performed with different styles and being able to shift between styles is a key skill for risk professionals as we must lead across a range of personality and group types.
- Good leaders typically have a keen understanding of relationships within quite large and complex systems and networks.

In summary, much of leadership can be counter-intuitive. For many risk professionals, leadership is often about "influencing" over "leading". Individuals and teams tend not to resist or push against something in which they have a strong involvement, ownership and sense of control.

Leaders of course need to be able to make tough decisions when required, but most importantly risk leaders should concentrate on enabling business teams to thrive, which is actually a 'sponsorship' or "coaching" role, not the dominant 'leading' role often associated with leadership.

Conclusion

The RMIA Master Class 2012 set out to explore the future for risk professionals in the converging world of governance, risk and compliance. The challenge was broken down into three elements:

- What GRC is and isn't.
- What are the implications for the role of the risk professional in leading the "G' in GRC?
- What capabilities and attributes do risk professionals need to lead and influence within a GRC environment?

While there was considerable debate on each of the issues, there was agreement that risk professionals can play a strong role in the evolution of a "risk centric" organisation, supported by an enterprise-wide approach to the management of risk. Deliberations throughout the session highlighted that there was a mature understanding of:

- The respective roles of each of the core components of ERM and GRC;
- The risk profession's historic successes and failures and the increasing need for strong leadership when the unpopular decisions need to be made;
- The extent to which the world is more transparent and connected than it has ever been, with the actions and philosophies of organisations scrutinised by the media and the general public as never before;
- The rapidly increasing awareness and interest in transparency and accountability of corporate governance and its many related concepts, such as social, community and environmental responsibilities.

In summary, many believe that this increasing scrutiny bodes well for risk professionals and we trust this discussion paper will encourage and assist others to take a strong lead in the future success of the organisations we serve.

References

1. Australian Institute of Management (2007) ***Manager Silent Obligations***
2. Chartered Secretaries Association (2012) ***What does a governance professional do?***
3. Corporate Integrity, LLC (2012), ***The evolving Role of a Chief Ethics and Compliance Officer***
4. Ernst and Young (2010), ***Aligning Corporate governance with ERM***
5. Institute of Directors, ***Business Risk – A Practical Guide for Board Members***
6. KPMG & CSA (2012) ***Governance Risk and Compliance***
7. OCEG, 2102 ***Risk Maturity Survey***
8. Open Pages White Paper, May 2008, ***"8 Principles of Risk Convergence and Implications for GRC Technology Solutions"***
9. PWC, ***Insights from the Boardroom 2012***
10. Warren Bennis (1989) ***"On Becoming a Leader"***

The Role of the Risk Professional in Leading the G in GRC

A discussion paper exploring the role of risk professionals in the converging world of governance, risk and compliance (GRC) to aid in understanding of how we may need to develop to grasp opportunities to lead organisations down the broader GRC path.

Why become a CPRM?

There are many answers to this question. First a CPRM designation provides recognition of your efforts to learn your craft, your commitment to self-development and your years of experience. It also flags to others you have been recognised within your profession to have attained high levels of expertise and competence. Finally, it provides you with access to high quality continuing education opportunities run by the RMIA exclusively for CPRMs. These opportunities include networking with CPRM peers who are also experts in their own fields of engagement in the risk profession.

RMIA
RISK Management Institution of Australasia

The Risk Management Institution of Australasia Limited (RMIA)