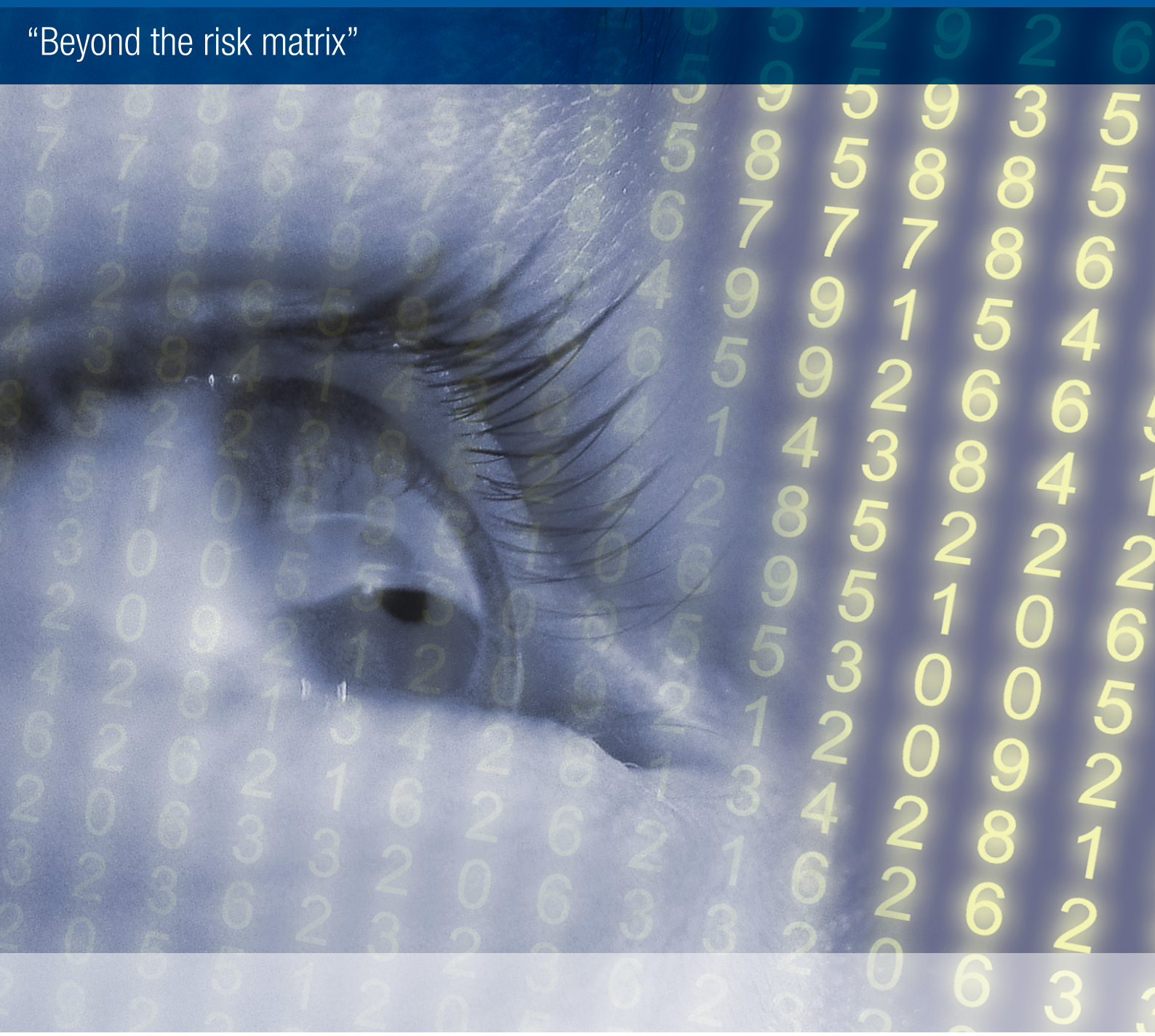
Effective risk assessment techniques

"Beyond the risk matrix"



Session 2 Discussion Paper
GRC 2012 Conference CPRM/CRMT Masterclass

RISK RMIA Management Institution of Australasia

The Risk Management Institution of Australasia Limited (RMIA)

Author:
Judy Clarey
Director RMIA Education & Professional Development

Facilitators:
Paul Chivers
RMIA Education & Professional Development Committee

Jeff Jones
RMIA Audit & Risk Committee

Moderator:
Sally Bennett
RMIA Director, Finance & Strategy

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 are drawn from a diverse range of industry, government and not-for profit sectors located predominantly in Australasia, with growing membership internationally.

The RMIA is committed to the recognition of professional competencies. Members with the relevant skill and experience can apply for accreditation at two levels - that of a Certified Practising Risk Manager (CPRM) or a Certified Risk Management Technician (CRMT).

About CPRMs and CRMTs

The CPRM and CRMT licence accreditation is based on a peer review process that requires members to demonstrate their knowledge and skills against a set of prescribed professional competencies.

As part of its commitment to professional development opportunities for members, RMIA coordinates a range of CPRM and CRMT networking and Masterclass workshops.

2012 Masterclass Acknowledgements

The RMIA would like to thank Jeff Jones (RMIA's Audit and Risk Committee), Paul Chivers (RMIA's Education and Professional Development Committee) and Sally Bennett (RMIA's Finance Director) for their time and efforts in developing and facilitating the GRC 2012 CPRM/CRMT Masterclass session.

A special vote of thanks is extended to:

- Chris Peace for making his research paper *"Effective risk Assessment – beyond the matrix"* available for workshop review;
- Members of RMIA's Education and Professional Development Committee;
- 2012 Masterclass participants for sharing their knowledge, experience and position on each topic.

Feedback from a survey of RMIA's Certified Practicing Risk Managers (CPRMs) conducted by RMIA's Education and Professional Development Committee (EPDC) early in 2012, indicated that there was a considerable amount of concern amongst risk professionals regarding the effectiveness of organisational risk assessment and analysis methodologies. In addition to the general unease around specific attributes of a given method, such as a qualitative versus quantitative approach, respondents indicated additional uneasiness with regard to:

- Reliance of executive and management teams on risk matrix-based tools and templates for the assessment of strategic as well as operational risks;
- Frequent use of a 'one size fits all' risk assessment matrix for business activities or projects;
- Difficulties experienced in convincing senior managers and supervisors that reliance on the Consequence/ Probability Matrix might in fact be limiting rather than enhancing their planning and decision making processes.

Further research by members of the EPDC, found that there were a range of discussion papers relating to the benefits and limitations of the 'risk matrix approach to risk assessment', including a 2012 conference discussion paper entitled ***"Effective risk Assessment – beyond the matrix"*** by Chris Peace (2012).

Chris Peace, a risk management consultant and Adjunct Lecturer in Management at the Massey University in Wellington, New Zealand kindly made his paper available for review by Masterclass participants.

This discussion paper provides an overview of the concepts and issues raised by Masterclass participants as well as a selection of "good practice" recommendations proposed during group discussion activities.

Methodology

This Masterclass session was designed to provide participants with the opportunity to share their ideas and experiences in relation to the challenge of **'taking the risk assessment process beyond the risk matrix'** and included the following topics and activities:

1. Introductory session to open discussion in relation to the strengths and weaknesses of **current risk assessment processes** facilitated by Paul Chivers;
2. A Case Study, based on a combined or **"triangulation" approach to project risk assessment** facilitated by Jeff Jones;
3. A Group Discussion Forum aimed at identifying **effective risk assessment techniques;**
4. Group feedback session on "**Good Practice" risk assessment recommendation** moderated by Sally Bennett.


“Beyond the risk matrix”

1.1 Risk assessment – A Value add approach?

Based on the simple premise that most organisations exist to create value for their stakeholders, then it follows that the 'objectives' of organisations are clearly established, and strategies put in place to achieve these objectives - which in turn are designed to create that 'value'.

In line with the definition of risk ***"as the effect of uncertainty on objectives"*** (ISO 31000:2009), these objectives are best set with a solid understanding of risks that could have either positive or negative effects, as well as the uncertainty around business forecasts and outcomes.

In his introduction to the session, Paul Chivers highlighted the fact there is evidence to suggest that in most organisations there is a vast amount of effort and resources invested in business planning and associated risk assessment processes. Ironically, many of these organisations report that there was often little to show in terms of "value add" - which is often compounded by the fact that for many organisations, the risk assessment process often has little to do with effectively managing the risks to "real business objectives" but instead is often driven by:

- Legislative and regulatory mandatory requirements—for example, workplace health and safety, environmental, financial requirements;
- "Tick the box" – compliance requirements;
- Funding requirements for specific projects or business initiatives;
- Validation of decisions that have already been made etc.

A recent OCEG Effective Risk Assessment Study (the Risk Study), sponsored by Ernst & Young, surveyed 250 companies on their approach to risk management to identify those that find value from their risk assessment processes. Eighty percent of the 250 participants in the Risk Study say their organisations are not getting as much value from their risk assessments as they should. They also indicated that they could increase value and protect it better, if they improved risk assessment techniques across a range of activities.

About half of the organisations surveyed use their risk assessments to evaluate operational and financial performance and to influence internal audit planning. Less than one third, though, use risk assessment to evaluate board or c-suite performance, define performance metrics, or challenge leadership decisions and business plans. Yet, when asked if these applications of risk assessment should be used, and if they would add or protect value, almost all say yes, and they are right. (OECG 2012)

> They fact that many admitted reliance on qualitative assessments over other evaluative means or modeling of any type indicates that their risk analysis results may well be little more than a hunch or "guesstimate" based on anecdotal information, so-called managerial intuition and limited direct information.. (OECG 2012)

According to the vast majority of participants in the study, the most apparent failing of the risk assessment process is the dependence on qualitative analysis above all else. While those who value their assessment process are nearly four times more likely to use quantitative techniques like net present value and statistical modeling, most study participants primarily rely on qualitative analysis techniques such as the consequence probability matrix in their evaluation of risk impact and most other factors.

1.2 Risk assessment - the 'Risk matrix" approach

Chivers provided an overview of Chris Peace's (2012) discussion paper ***"Effective risk Assessment – beyond the matrix"*** as a lead into group discussion around the application and effectiveness of current "risk assessment processes and practice".

The findings in relation to current risk assessment practice outlined in Peace's discussion paper are based on a survey of risk practitioners over a 12 month period. The survey highlighted that:

- There was no agreed **definition of risk assessment**, for example, the terms ***quantitative risk analysis*** and ***quantitative risk assessment*** **(QRA)** being used to mean the same thing - which If we accept that **risk assessment** is "the overall process of risk identification, risk analysis and risk evaluation" as defined in the International Standard ***ISO 31000:2009***, the latter **QRA** method would give rise to the need to carry out quantitative risk identification and evaluation, neither likely to be achievable;
- Often, the risk analysis processes do not use techniques that provide more detailed information about risk events, consequences and their associated likelihoods; uncertainty may not be adequately considered and impacts on objectives not fully understood;
- Many risk assessments are based on a simple analysis using a 5x5 matrix or similar as a tool for ranking and displaying risks by defining ranges for consequence and likelihood. Peace (2012) proposes that such analyses may lack understanding of the organisational context and relevant risk criteria, and naming of risks may fail to describe them in adequate detail.
- Simplistic application of a matrix can lead to the false impression of certainty about a consequence or its likelihood or both when there are, in fact, a range of consequences or likelihoods or both. In other words, there is uncertainty about the impact on objectives of a given risk event.

Peace (2012) highlights some problematic features of risk matrices previously outlined by Cox (2008) as:

- **Poor Resolution.**
  Typical risk matrices can correctly and unambiguously compare only a small fraction (e.g., less than 10%) of randomly selected pairs of hazards. They can assign identical ratings to quantitatively very different risks ("range compression").
- **Errors.**
  Risk matrices can mistakenly assign higher qualitative ratings to quantitatively smaller risks. For risks with negatively correlated frequencies and severities, they can be "worse than useless," leading to worse-than-random decisions.
- **Suboptimal Resource Allocation.**
  Effective allocation of resources to risk-reducing countermeasures cannot be based on the categories provided by risk matrices.
- **Ambiguous Inputs and Outputs.**
  Categorizations of severity cannot be made objectively for uncertain consequences. Inputs to risk matrices (e.g., frequency and severity categorizations) and resulting outputs (i.e., risk ratings) require subjective interpretation, and different users may obtain opposite ratings of the same quantitative risks.

These limitations suggest that risk matrices should be used with caution, and only with careful explanations of embedded judgments. In addition, Cox also draws our attention to the fact that:

> "Even if a matrix has been well designed and takes account many of these factors, there has been very little rigorous empirical or theoretical study of how well risk matrices succeed in actually leading to improved risk management". (Cox 2008)

1.3 Risk Assessment – A "justifiable" approach?

During his presentation, Chivers proposed that as risk professionals it is our duty to assess risks to a depth that is "justifiable" – an essential element, he believes is often overlooked during the risk assessment process. According to Chivers, due diligent risk assessment should be able to answer the following fundamental questions:

- What can happen and why (by risk identification)?
- What are the consequences?
- What is the probability of their future occurrence?
- Are there any factors that mitigate the consequence of the risk or that reduce the probability of the risk?

A "justifiable" risk assessment process according to Chivers is determined by asking three questions.

- Is it justifiable in an international court of law?
- Is it justifiable under peer review?
- Does it address the effect of uncertainty on the objective?

The concept of "justifiable" risk assessment process provided the catalyst for group discussion on the purpose and intent of the risk assessment process. During these discussions, there was general consensus that as practitioners, we often have a preference towards risk assessment techniques due to our experience, subject matter expertise and available resources.

Peace (2012) suggests that this 'preference' is really a "confirmation bias", a type of cognitive bias that can influence the selection of risk assessment tools and techniques that we feel most comfortable with. He proposes that there is evidence to support that some practitioners actively seek out and assign more weight to tools and evidence gathering techniques that confirm their hypothesis, and ignore or underrate evidence to the contrary.

According to Peace (2012), experience shows that risk assessments in many organisations are largely poorly designed with little relationship to the risk profile of the organisation. Other considerations include:

- Information provided by risk analyses may be limited to "snapshot" views of consequences and their likelihoods derived from the experiences of a few people;
- Decisions about acceptance and treatment of risk may then be made using inadequate information. It comes as no surprise that some, perhaps many, decisions may subsequently be found to have been ill-informed;
- Simplistic application of a matrix can lead to the false impression of certainty about a consequence or its likelihood or both when there are, in fact a range of consequences and likelihoods or both;
- Risk assessments need to use the best available information, by systematic, structured and timely and go beyond simplistic application of risk matrices. They have to address uncertainty and take human and cultural factors into account;
- In addition to being tailored to the specific needs of an organisation, they need to be transparent to enable evaluation and regularly updated in the light of changes in the context.

Which, according to Chivers begs the question, "Are the risk assessment tools selected and the information gathered truly justifiable?"

1.4 Risk Assessment – A combined approach

Peace (2012) advocates that if "risk management is to be part of decision making" (Principle c, paragraph 3, ISO 31000) it is essential to provide somewhat more information than the level of risk from the likelihood of one consequence. Indeed, providing a range of consequences and their associated likelihoods will be but part of a risk analysis. Several techniques might be required to adequately "comprehend the nature of risk and to determine the level of risk" from a new technology, major natural disaster, disruption of a supply chain or major loss of containment.

Workshop participants were invited to review the international standard IEC ISO 31010:2009 *Risk Management — Risk Assessment Techniques.* This International Standard is a supporting standard for ISO 31000:2009 and provides guidance on selection and application of 31 systematic techniques for risk assessment, 14 of which are "strongly applicable" to risk identification, and 22 techniques that are "strongly applicable" to risk analysis regardless of the nature of the risks.

There was much discussion on the benefits of combining two or more different risk assessment techniques (triangulation) and it was widely acknowledged that where accurate and timely data is available, qualitative analysis should be supported by more rigorous quantitative techniques — ranging from benchmarking to probabilistic and non-probabilistic modelling.

Peace (2012) provides an example of a combined approach from his risk assessment work with a transport-related organisation. During semi-structured interviews to identify project related risks, concerns were raised by several people about the effects of changing fuel prices and possible consequences related to altered vehicle use. This led to application of SWIFT and the identification of a wide range risks associated with both increased and reduced costs of oil-based fuels that had not previously been considered. (Peace 2012)

2.1 Risk Assessment – a "triangulation" approach

Based on the premise that the best risk assessment methodology should use a combination of approaches in order to capture all that is known and as much as possible about what is not known, Jeff Jones provided an overview of a 'triangulated risk assessment technique" he had utilised during a recent oil and gas industry project. The assessment techniques were based on a combination of a Monte Carlo Simulation process combined with a matrix based qualitative and quantitative risk assessment methodology. In this case, the combined techniques were used to help define the appropriate amount of Owner's Cost Contingency for the effective delivery of the project.

Jones explained that the Monte Carlo simulation, or probability simulation, is a technique used to understand the impact of risk and uncertainty in financial, project management, cost, and other forecasting models.

To that end, when you develop a forecasting model – any model that plans ahead for the future – you make certain assumptions. These might be assumptions about the investment return on a portfolio, the cost of a construction project, or how long it will take to complete a certain task. Because these are projections into the future, the best you can do is estimate the expected value and an MC model can help review a probabilistic view of the range of possible outcomes, to assist decision making and managing uncertainty.

2.2 Risk Assessment - What can a Monte Carlo Simulation tell you?

According to Jones in some cases, it is necessary to estimate a range of values. In a construction project, you might estimate the time it will take to complete a particular job; based on some expert knowledge, you can also estimate the absolute maximum time it might take, in the worst possible case, and the absolute minimum time, in the best possible case. The same could be considered for project costs. In a financial market, you might know the distribution of possible values through the mean and standard deviation of returns. By using a range of possible values, instead of a single guess, you can create a more realistic picture of what might happen in the future.

This is different from a normal forecasting model, in which you start with some fixed estimates – for example- the time it will take to complete each of three parts of a project – and end up with another value – the total time for the project. If the same model were based on ranges of estimates for each of the three parts of a project, the result would be a range of times it might take to complete the project. When each part has a minimum and maximum estimate, we can use those values to estimate the total minimum and maximum time for a project.

Following on from the previous risk assessment and case study discussions, workshop participants were divided into four groups with a view to identifying risk assessment tools or techniques that they would recommend be used to support or build on commonly used Consequence /Probability risk matrix techniques. The risk assessment categories allocated to the groups were:

1) Strategic;

2) Operational;

3) Project;

4) HSE risks

Group 1 Strategic Risk Assessment Techniques

This group discussed techniques suitable for strategic risk assessment and recommended techniques that were suitable for assessment at two levels:

For **immediate or current strategic** risks the preferred assessment techniques included:

- **Stakeholder Analysis** using a variety of tools on both qualitative and quantitative data to understand stakeholders, their positions, influence with other groups, and their interest in a particular area.
- **"Political, Economic, Social, and Technological analysis"** which is used in the review of macro-environmental factors used in the environmental scanning component of strategic risk analysis management – often with **Environmental and Legal** factors included – which extends the framework acronym to ***PEST – EL.***
- **Porter's Five Forces Competitor Analysis** is a risk assessment framework for industry analysis and business strategy development formed by Michael E. Porter of Harvard Business School in 1979. It draws upon industrial organisation (IO) economics to derive five forces that determine the competitive intensity and therefore attractiveness of a market. Attractiveness in this context refers to the overall industry profitability. An "unattractive" industry is one in which the combination of these five forces acts to drive down overall profitability. A very unattractive industry would be one approaching "pure competition", in which available profits for all firms are driven to normal profit.

Listed below are the groups' recommendations for **future proofing – "over the horizon"** strategic risk assessment techniques focused on business sustainability and resilience – risk assessment techniques that are based on the premise that strategic analysis and decision making needs to be based on key risk indicators (KPIs).

- **The Frog in a Beaker** or Boiling Frog analogy was used to summarise the group's thinking and discussion on the importance of performance based business improvement and change management strategies. **The boiling frog** story is a widespread anecdote describing a frog slowly being boiled alive. The premise is that if a frog is placed in boiling water, it will jump out, but if it is placed in cold water that is slowly heated, it will not perceive the danger and will be cooked to death. The story is often used as a metaphor for the inability of people to react to significant changes that occur gradually.
- **BHAG analysis** without considering likelihood. The term 'Big Hairy Audacious Goal' (BHAG) was proposed by James Collins and Jerry Porras in their 1994 book entitled *Built to Last: Successful Habits of Visionary Companies.* A BHAG encourages companies to define visionary goals that are more strategic and emotionally compelling. Many businesses set goals that describe what they hope to accomplish over the coming days, months or years. These goals help align employees of the business to work together more effectively. Often these goals are very tactical, such as "achieve 10% revenue growth in the next 3 months."
- **Points of Failure Analysis** - based on a methodology for identifying and eliminating problem root causes, and specifically, the root causes of complex systems failures.
- **Scenario analysis** is a process of analysing possible future events by considering alternative possible outcomes (sometimes called "alternative worlds"). Thus, the scenario analysis, which is a main method of projections, does not try to show one exact picture of the future. Instead, it presents consciously several alternative future developments. Sets of scenarios reflecting (for example) 'best case', 'worst case' and 'expected case' may be used to analyse potential consequences and their probabilities for each scenario as a form of sensitivity analysis when analysing risks at strategic level.

Group 2 Operational Risk Assessment Techniques

Much of the discussion for this group centred on the risk assessment techniques commonly practiced by public sector, local government and not-for-profit agencies. The establishment of risk assessment techniques linked to overarching business was dependent on:

- The alignment of agency vision and goals with divisional goals and objectives;
- Clear objectives and measurable performance indicators;
- Contextualised risk analysis and evaluation criteria;
- "Fit-for-purpose" tools that allowed for clear documentation of assessment objectives and scope, assumptions, limitations, risk rankings, treatment priorities, actions and accountabilities;
- Cost benefit /and or Business Impact Analysis techniques used as required to prioritise treatments;
- Clear accountability for resourcing implementation, review and reporting requirements.

There was agreement on the fact that the risk assessment techniques often used by these organisations was often dependent on:

- Risk assessment skills, experience and capability of the risk assessment team;
- Constraints on time and other resources within the organisation;
- The budget available if external resources are required.

With this in mind the group recommended the use of:

Brainstorming – because it can be used in conjunction with other risk assessment methods or may stand alone as a technique to encourage imaginative thinking and risk identification at any stage of the risk management process. It may be used for high-level discussions where issues are identified, for more detailed review or at a detailed level for particular problems. It is therefore particularly useful when identifying risks associated with new technology, new projects, where there is no data or where novel solutions to problems are needed.

Delphi Technique

The Delphi technique is a procedure used to obtain a reliable consensus of opinion from a group of experts. Although the process is often used to mean brainstorming, an essential feature of the Delphi technique, as originally formulated, was that experts **expressed their opinions individually** and anonymously while having access to the other expert's views as the process progresses. The Delphi technique can be applied at any stage of the risk management process or at any phase of a system life cycle, wherever a consensus of views of experts is needed.

Strengths include:

- as views are anonymous, unpopular opinions are more likely to be expressed;
- all views have equal weight, which avoids the problem of dominating personalities;
- achieves ownership of outcomes;
- people do not need to be brought together in one place at one time;
- Eliminates bias, “leader following”, or collective group thinking tendencies.

Limitations include:

- it is labour intensive and time consuming to set up;
- participants need to be able to express themselves clearly.

Group 3 Project / Concept Proposal Risk Assessment Techniques

The group readily acknowledged that the consequence /probability matrix was a commonly used project risk identification and screening tool because it was relatively easy to use, and if well designed and applied could be used at all stages of a project to determine if risks:

- are acceptable or not acceptable based on pre-determined appetite and tolerance criteria that align with the objectives of the project;
- require more detailed information or additional analysis;
- need additional treatment / controls;
- should be referred to a higher level of management;
- require no further consideration at this time.

It was also acknowledged that the risk assessment process should involve more than simply listing identified risks and prioritizing them by their probability of occurrence and impact on objectives. The large amount of risk data gathered prior to, and produced during the project must be structured so that we can understand it and use it as a basis for action.

In essence it is important for organisations to acknowledge that risks in projects are complex - arising from a wide range of sources and having a broad scope of possible impacts - so the risk matrix format, definitions and the discipline applied to it are totally dependent on the context in which it is to be used.

Group 4 HSE Risk Assessment Techniques

As all organisations in Australia have legislative and common law obligations to have arrangements in place to cover their management of health, safety and the environment - it was readily acknowledged that **robust risk assessment techniques** are integral to the success and effectiveness of any health and safety and environmental management systems hereafter referred to as the **HSEM**.

There was also consensus on the fact that an effective **HSEM** should provide a systematic way to identify hazards and effectively control risks to a level that is as low as is reasonably practicable /achievable. Ideally the HSEM should be:

- Driven by a ***Board endorsed HSE Policy commitment*** to zero harm of people, product, process and the environment;
- Based on business based goal setting, planning, performance measurement and reporting processes as determined by the Board – ***"What does the Board want to know?";***
- Reflect the complexity of business activities and working environment;
- Systematic, explicit and comprehensive process that are implemented, resourced and reviewed by ***"capable" and accountable managers;***
- Integrated into the overarching management system that supports organisation's business activities and be ***"Woven into the fabric of an organisation"***
- ***"Part of the culture, the way people do their jobs."***

Group discussion also highlighted a range of **HSE** related international and national industry specific standards many of which are predicated on the Plan Do Check Act (PDCA) quality /business improvement principles and frequently used as the framework elements for many HSE management systems. For example:

Quality Management Systems (QMS)

- ISO 9001
- AS9100 (Aircraft, Space & Defence)

Environmental Management Systems (EMS)

- ISO 14001

Occupational Health & Safety (OHSMS or SMS or HMS)

- OHSAS 18001:2007
- AS/NZS 4801: 2001

In summary, all HSE systems today are based on risk assessments that require varying degrees of depth and detail. The form of the assessment will **"depend"** on the complexity of the decision making and output required. This in turn will determine whether the risk needs to be evaluated using quantitative, semi-quantitative or qualitative criteria – which can used in a range on commonly used risk assessment techniques such as:

1. **Informal risk assessment** (RA) identification & communication of hazards & risks in a task by applying a way of thinking, e.g. checklists and observation techniques - often with no formal documentation;
2. **Job safety/hazard analysis** (JSA/JHA)—identification of hazards & controls in a specific task, usually for determining standard work practice;
3. **Preliminary hazard/risk analysis/** Workplace Risk Assessment and Control (PHA/WRAC)—identification and analysis of risk issues/events, often to determine the need for further detailed study;
4. **Hazard & operability study** (HAZOP)—systematic identification of hazards in a process plant design;
5. **Fault tree analysis** (FTA)—detailed analysis of contributors to major unwanted events, potentially using quantitative risk analysis methods;
6. **Event tree analysis** (ETA)—detailed analysis of the development of major unwanted events, potentially using quantitative methods;
7. **Failure modes, effects and criticality analysis** (FMECA)—general to detailed analysis of and other potential consequence areas.

4.0 General findings and "Good Practice" recommendations:

Very early in the workshop robust discussion and debate arose on the subject of "what was driving the approach to the risk management techniques and processes used in many organisations today". There were those who proposed that the key driver of the risk assessment process in their organisations was primarily about **"informed decision making"** on business outcomes - and others who were of the strong opinion that in spite of the AS/NZS ISO 31000 rhetoric espoused by many organisations the key driver was that of **"backside protection"** – with a focus on justification or **"defence"** of management decisions and actions to be taken or in many instances justification for decisions that had already been made.

Interestingly, despite some initial polarisation of opinion on what is driving current practice and process in some organisations - it was obvious that there were many risk professionals in the room who worked with organisations who clearly "got the message" that the risk matrix assessment methodology was not a "one size fits all" or a "one stop shop" solution – but rather an "enabler" that when designed to suit the context, could serve as a tool to aid in both the preliminary or "first pass" estimation and ranking of risks as well as the longer term monitoring and review of risks associated with specific business outcomes.

4.1 Common Pitfalls – recommendations for improvement

There was also shared concern and consensus on the some of the common pitfalls associated with current risk assessment processes across industry. The recommendations for improvement of the risk assessment process discussed during the workshop appeared to fall into two main categories namely:

4.1.1 Stakeholder and Relationship Management

Getting the right people/stakeholders involved in, and accountable for the risk assessment process. In particular the need to involve people with:

- the knowledge and understanding of the business activity or process being assessed;
- a business improvement mindset, rather than a "defensive" negative approach;
- an understanding of the relevant compliance requirements;
- the ability to engage the right stakeholders by talking the right "language";
- a knowledge of the culture and risk appetite of both the stakeholders and the organisation;
- the responsibility and capability to drive the process beyond a Matrix-based assessment as required;
- accountability for allocating resources to the process and its outcomes;
- the ability to communicate the outcomes to the right stakeholders.

4.1.2 Alignment of Risk Strategy with Business Strategy

It was generally agreed that most organisations in Australia may be able to demonstrate that they have in place core risk assessment processes (e.g. identification, analysis, evaluation and treatment processes) that align with AS/NZS ISO 31000. However, discussion centred on the fact that risk assessment processes in some organisations were not sufficiently aligned with all five of the risk management process elements. They were often not aligned with business outcomes of the organisation, and worked well in some parts of the organisation or for some projects or activities but not in others. Misalignment of risk management practice and business strategy is often based on a failure to establish:

- **Strong and sustained commitment** to risk policy and process by the Board and Senior management;
- Clearly articulated and **communicated business outcomes,** risk appetite and associated KPI's;
- Enhanced leadership capabilities that include the ability to understand **human behaviour** and **influence organisational culture.**

In essence, if the risk management system or **"discipline"** is to support the risk assessment process the organisation, then it should also be dependent on:

a) understanding the organisation or business context, as well as

b) effective communication and consultation with relevant stakeholders.

4.2 "Good Practice" Recommendations

It was recognised that key enablers to effective risk assessment should be based on techniques that are:

- Contextualised – made "fit for purpose" for specific industry and business needs;
- Based on the best available information from multiple sources and techniques;
- Systematic, structured (disciplined) and timely processes that go beyond simplistic application of risk matrices;
- Transparent, well communicated in the language of the stakeholders;
- Supported by a strong "modeled" leadership and practice from the Boardroom down;
- Facilitated by competent practitioners who are cognisant of impact on the process by human behavioural and cultural factors;
- Well documented, accessible, repeatable and regularly updated in the light of changes in the context.

Key Learnings and Concluding comments:

For risk assessments to yield meaningful results, certain key principles must be considered:

- The risk assessment process should begin and end with specific business objectives based on key value drivers.
- Governance over the risk management should be clearly established - one that is based on the overall risk appetite and tolerance which are reflected in leading indicators designed to anticipate possible risks and opportunities before they materialize.
- The risk assessment discipline evolves and matures over time. Organisations typically start with broad, qualitative risk assessment criteria, then gradually refine their assessment and analysis techniques, as they establish, test and monitor relevant evaluation criteria and performance indicators, specifically aimed at supporting informed decision making and allocation of resources.
- In organisations that are early in the risk maturity journey, the risk matrix is most commonly used, building a common language, with little or no thirst for more detailed information and analysis. Risk assessment and analysis methodologies especially in the qualitative space may be flawed if they are not tailored to specific objectives and outcome. Evidence-based risk assessment can help relieve some of the growing pains.
- In more mature organisations, the risk matrix is strongly supported by more detailed risk assessment techniques that are informed by an integrated information management system. For these organisations enhanced 'information management', will continue to be core to the evolution of their overall assurance approach to risk management.

In conclusion, risk management is not "a silver bullet." There is not one single risk assessment process to rule them all. Different valid approaches exist, just as there are different sources of risk, risk information and data. (Tomhave, 2010).

References

1. AS/NZS ISO 31000: 2009– **Risk Management Principles and Guidelines**
2. Cox LA Jr. 2008; ***What's wrong with risk matrices?*** Cox Associates and University of Colorado, 503 Franklin St., Denver, CO 80218, USA. tcoxdenver@aol.com
3. Hubbard Larry (2011) ***The Matrix Revisited***
4. IEC ISO 31010:2009 – ***Risk Assessment Techniques***
5. Internal Auditor Risk Watch Column, April 2009 Issue
6. Tomhave Benjamin (2010) ***Maddening Methods: Fundamentals of Risk Assessment and Analysis;*** ISSA Journal, July 2010
7. OCEG (2012) ***Identifying Value-Added Risk Assessments:*** Preliminary Findings of the OCEG Effective Risk Assessment Study, http://www.oceg.org/view/20057
8. Peace Chris (2012) ***Effective risk Assessment – beyond the matrix***
9. Price Waterhouse Coopers (2008) ***"A practical guide to risk assessment"*** pwc.com/us/grc

RISK Management Institution of Australasia

The Risk Management Institution of Australasia Limited (RMIA)