A U S T R A L I A N N A T I O N A L A U D I T O F F I C E

Risk Management Institution of Australasia

ACT Chapter Conference
"Building on Experience"

RISK IS ALL AROUND

24 September 2010

With thanks to Ron Richards of my Office
for his assistance in the preparation of this address

Ian McPhee, PSM
Auditor-General for Australia

I Introductory Remarks

Thank you for your invitation to be the keynote speaker at the RMIA's ACT Chapter conference. The conference theme 'Building on Experience' is very timely as there is no area of commercial or government endeavour which has been more profiled by recent economic events, or issues in public sector program delivery, than risk management.

Risk **is** all around.[1] Risk is unavoidable in our personal lives and in the business environment and, increasingly, a level of risk taking is necessary to achieve goals as well as governments' policy objectives efficiently — **but** it must be managed.

Organisations with sound risk management processes seemed to have better survived the global financial crisis, particularly those with a strong risk culture combined with effective governance arrangements. In essence, a sharp focus on three 'lines of defence' — leadership from top management, a sound risk management function and an effective audit function. These 'lines of defence', staffed with capable people imbued with a strong sense of risk awareness, are at the heart of effective risk management.[2]

David Murray, Chairman of the Future Fund and former CEO of the Commonwealth Bank, at a recent APEC lecture, suggested that those who practiced rigour and had a scientific approach to calculating risk were more likely to have systems in place which mitigated the adverse effects of the GFC.[3]

The President of RMIA, Brian Roylett, was reported as saying that many organisations have failed to adopt effective enterprise-wide risk management cultures and behaviours, adding fuel to the global financial crisis. However, he went on to observe: '*there has been no systemic failure of risk management as a business discipline. Perhaps we have failed risk management*'.[4]

The message here is that we are well placed with effective standards, including the relatively new AS/NZS risk standards. But we have much to do in converting the theory into sound practice.

This leads me to the central tenet of my presentation today — the importance of implementing risk management effectively to avoid the failures in risk management that commonly flow from poor implementation approaches or a failure to monitor the changing environment, and respond accordingly.

The second key message in my presentation today is that the management of risk must be embedded in an organisation's modus operandi – in its corporate planning, reporting, decision making and management practices. Organisations need to encourage and grow a culture of risk management within an organisation; it should be part of day-to-day business and not a 'one off' activity; and the leadership group, through its actions, must show the way.

Thus, for success, risk management must become a part of the management process applied to all aspects of the organisation's business and part of everyone's responsibilities. And this is true for the public sector as it is for the business sector.

Against this backdrop I propose to examine the practice of risk management in the public sector to see what we have learned, and emerging influences we need to take account of in implementing government programs as we go forward.

II Risk Management in the Public Sector

The very encouraging aspect of public sector management today is that the importance of risk management is recognised. This wasn't always the position.

I think it is fair to say that, in the public sector, Pat Barrett AO, former Auditor-General and senior Finance executive, did more than anyone to put risk management on the public sector management agenda in the 1980s. Well-placed to see the opportunities to integrate a better understanding of risk management with reforms designed to *'let the managers manage'* and *'make the managers manage',* Pat strongly promoted the benefits of risk management to a population of public servants then used to working in a more rules based world. He saw the need to complement the devolution and greater flexibility being accorded to public sector agencies with a better understanding of sound management practices, particularly risk management.

As each year passes, the business environment is becoming more complex. The world doesn't stand still. And boundaries between previously discrete organisations, organisational units and functions are becoming more porous. This means that projects and programs need to deal with a greater level of inter-connectedness and all of the technological enablers. So, while the fundamentals of project management may not change significantly, the risks to successful implementation are higher due to the more complex nature of our environment and the extent of uncertainty.[5]

As we know it today, risk management is a structured approach to allow organisations to manage risks to a level assessed as being appropriate to the organisation's risk appetite.

- Risk is characterised by uncertainty, in that the 'consequences' and 'likelihood', which form the basis of the risk assessment, may not be known with any precision.
- Elimination of risk is generally not a practical goal, but risk can be managed and mitigated by various treatments.

As a minimum, risk management should be applied at the enterprise level, the divisional level and the project level.

- it is no longer discretionary
- it is an integral part of good management – like strategic planning, project management, supervision, and so on.

We have to be willing to invest in risk management and risk intelligence. Risk management needs to be strongly supported by those in leadership positions because it is one of those disciplines, if done well, will generally not be visible for all to see. Sadly, only risk management failures attract attention, and headlines. Thus, an organisation's leadership needs to compensate for this asymmetry by reinforcing the positive outcomes of risk management action.

If risk management were straightforward, then public sector programs would be designed, implemented and administered successfully in a fairly mechanistic way – but we know there is more to successful risk management than that.

I imagine all of us have been in situations where risks could have been better managed.

We know, on the basis of our observations and experience, it doesn't pay to be over-confident in assessing an organisation's ability to manage risk.

One of the most illuminating examples of the importance of active risk management, quoted in a publication by Arthur Anderson: *Managing Risk, Managing Value,* [6] was the comment by Rick Buy, Executive Vice President and Chief Risk Officer, Enron in 2000:

> *A rattlesnake may bite us every now and again, but we knew it was there and how much it might hurt.*

If only we could assess the likelihood and consequence of risks so clearly and confidently. Perhaps the lesson here is not to be over-confident like the Enron executive, but to actively monitor risks, as neither Enron nor Arthur Anderson has survived.

Today, in our various official roles, there is an expectation that we will take steps to manage the risks of inadvertent events or poor processes. We are also expected to consider opportunities which we can convert to our advantage – the other side of the risk coin.

The firms that avoided significant fallout from the global financial crisis demonstrated a comprehensive approach to viewing firm-wide exposures to risk; shared quantitative and qualitative information more efficiently across the firm; and engaged in more effective dialogue across the management team. They had more adaptive (rather than static) risk measurement processes and systems that could rapidly alter underlying assumptions to reflect changing circumstances. Management also relied on a wide range of risk measures to gather more information and different perspectives on the same risk exposures with more use of scenario analysis. In other words, they exhibited strong governance systems with the information being passed upwards to the board.[7]

The key findings of a global risk management survey (the Deloitte Global Risk Management Survey: Sixth Edition) are very helpful in highlighting not only the current state of risk management but also in providing pointers to factors which contribute to sound approaches which apply, or could be adapted to apply, in the public sector:

- Risk management is not fully integrated throughout many institutions: 49 % of the institutions surveyed had completely or substantially incorporated responsibilities for risk management into performance goals and compensation decisions for senior management.

- Overall responsibility for oversight and governance of risks rested with the board of directors at 77 % of the institutions participating, and 63 % of these had a formal, approved statement of risk appetite.

- 73% of the institutions surveyed had a Chief Risk Officer (CRO) or equivalent position. As an indicator of the role's importance, the CRO reported to the board of directors and/or the CEO at roughly 75% of these institutions.

- Only 36 % of the institutions had an enterprise risk management (ERM) program, although another 23 % were in the process of creating one. Among institutions with $100 billion or more in assets, 58 % had an ERM program already in place. The institutions that had ERM programs found them to be valuable: 85 % of the executives reported that the total value (both quantifiable and non-quantifiable) derived from their ERM programs exceeded costs.

- Roughly 75% of the institutions had fully completed or substantially completed the work required to identify operational risk types, and to standardize the documentation of processes and controls for operational risk. Yet, only roughly 40 % of executives considered their operational risk assessments and their internal loss event data to be well-developed.

- Many institutions may have significant work to do to upgrade their IT risk management infrastructure.[8]

The Deloitte commentary on the survey drew the conclusion that beyond methodologies, data, and technology capabilities, the effectiveness of risk management may require enhancing or, in some cases, creating a pervasive risk-aware culture throughout the organisation—and creating an environment and incentives that sustain this culture over time.

Another of the Big 4 accounting firms, Ernst & Young, has also provided a report[9] on 'the top 10 risks for business' following interviews with industry executives and analysts. I found the business risk radar, set out below, a particularly useful way to structure the consideration of the full range of business risks.

Source: Ernst & Young, Australia. *The Ernst & Young Business Risk Report 2010 – The top 10 risks for global business.*

With minimal change, this risk radar could be modified to suit the particular purposes of public sector agencies, e.g. the strategic focus could readily be amended to accommodate the risks to the appropriateness of current policy settings.

One of the complementary benefits of the stronger focus on risk management by boards and senior management has been an increased focus on internal audit, as recently pointed out by Gary Anderson, MD Protiviti:

> '*Interest in internal audits has increased in step with the rise in interest in risk management, as internal audits provide independent assurance of the effectiveness of a company's risk-management practices and internal controls.*'[10]

I was also amused to see a recent press headline *Risk managers 'the new black' as hiring soars* as many financial services firms add risk assessment positions to more divisions following the global financial crisis.[11]

As you know, the ANAO, through its work, gets to see examples of risk management done well, and done not so well. Unfortunately it is not just a case of saying there are '*x*' factors that are critical to success and focus on these, because there is a good chance the other factors you thought were under control will unravel.

In assessing and managing risk, we need to keep all dimensions in view, or on the radar screen.

Whatever the task – policy design, implementation, program administration - it is really a case of understanding the fundamentals of good management, of which good risk management is an essential part:

- Understand the context, the goal, strategies, and what success will look like;
- Know how to effectively resource the mission; allocate responsibilities; and be willing to hold those responsible to account;
- Determine scorekeeping arrangements, with an accent on unexpected variations;
- And overlay this with a sound approach to risk management, including an understanding of risk tolerance.

And, when doing this, reflect on the strengths and weaknesses of your organisation to deliver a sound result. I call this organisational 'self-awareness'. Be sure to compensate for any weaknesses arising from your analysis.

The ultimate goal for all organisations is to build risk management into the organisational culture so that we have better performing and more resilient organisations.

As touched on earlier, making management decisions in critical areas presumes we have an understanding of risk tolerance.

Broad statements about the APS being 'risk averse' are not that helpful as risk tolerance varies in the APS, depending on the type of functions being administered and the stakeholder population.

There will be legitimate instances where a low risk tolerance will be appropriate. Some of these instances may be driven by legislative, policy or other ministerial requirements.

Mark Matthews [12] of the Australian National University has observed that public sector decision-making can appear cumbersome, risk averse and time consuming because the unintended consequences of getting it wrong are far too severe. He makes the point that it is dangerous to react to such criticism defensively; and the reality is that governments handle uncertainties and risks that markets can't cope with.

So the message here is to set the organisational risk appetites to reflect the circumstances, but also be willing to re-assess risk tolerances. In some circumstances, such as implementing an IT system or acquiring a major item of plant, our risks appetite might be comparable with the private sector, but in advising on, and implementing a new policy measure, greater caution is understandable because of the consequences for key stakeholders of a public sector agency misqueuing.

We would all accept, nevertheless, that there are cases where we could operate more efficiently by more effectively managing risks than following boilerplate approaches. If policy and legislation requires such an approach, and it is considered unduly constraining or resource intensive, we should inform the responsible policy department to consider modifying the approach that is stipulated.

There are many ways to attune your antenna to risk situations that may need close oversight. For instance, the Standish Group has, for many years, published the factors that contribute to successful project management[13]:

User Involvement

Executive Support

Clear Business Objectives

Emotional Maturity (managing over-ambition)

Optimisation (managing over and under building)

Agile Process

Project Management Expertise

Skilled Resources

Execution

Tools and Infrastructure

You can also talk to colleagues, read relevant review reports and audit reports.

Our work shows some commonality with the Standish factors. Specific audits have highlighted a number of other factors that are worthy of agencies' attention:

1. Know your organisational responsibilities in a joined-up world

- In today's world, where achieving better outcomes relies on more effective relationships between the Commonwealth and the States/Territories, central agencies and line agencies, and central and regional offices, it is critical to know 'who is responsible for what'.
- It is also important to understand where the chickens will come home to roost if risks aren't managed effectively by one of your 'partners'. This might be called contingency planning, and increasingly for politically sensitive programs, it is a wise investment for public sector agencies.

2. The role of management:
   - It is critical that managers have ownership of their responsibilities, and are actively involved in risk management from the design of the proposal for a policy measure through to its implementation. This includes being aware of leading indicators of issues arising and guiding any extraordinary action. We have noticed in more than one recent audit that senior management considered their responsibilities had been discharged by offering extra support as required, but not really understanding a range of matters that suggested the program was far from being on track.
   - In a similar vein, the *Final report of the 2009 Victorian Bushfires Royal Commission* commented in some detail on 'the fundamental responsibility of those in command'. The Commission very much supported the idea of an active leader and active management in the context of the matters before the Commission.
   - The following extracts from the Commission's report go to this point:

> "The Commission observed a disturbing tendency among senior fire agency personnel – including the Chief Officers – to consistently allocate responsibility further down the chain of command, most notably to the incident control centres.[14]
>
> "Mr Rees (Chief Officer, Country Fire Authority) justified his delegation of IMT supervision by saying he risked "losing focus" if he drilled down into the detail of any particular fire."[15]
>
> "On 7 February Ms Nixon took a 'hands-off' approach to her responsibilities as State Coordinator of the State Emergency Response Plan . . ."
>
> "Ms Nixon considered that her leadership functions were discharged by establishing a competent team and being available if needed. But on a

> day when conditions were predicted, and then proved, to be worse than Ash Wednesday something more was required."[16]

- Clearly these comments by the Commission relate to particular circumstances of an extreme emergency. Nevertheless, there are some important pointers here for public sector managers in relation to community expectations – take responsibility, calibrate your direct involvement in program management to the significance of the issues arising but, importantly, roll your sleeves up when things aren't going to plan.

3. Understanding, and adhering to, the legislative and policy framework:
   - It almost goes without saying that agencies are expected to understand the legislative and policy dimensions of programs they are responsible for administering, and for advising Ministers, as appropriate, in this respect.
   - Re this latter point, it is not surprising that, from time to time, Ministers need to be informed of any legal or policy responsibilities they should be taking account of in decisions, as they commonly make decisions across a wide spectrum of issues and should be informed of any 'constraints' that bear on those decisions.

4. Having the right horse-power for the task:

   - If the task is important enough, get the right people, and enough of them, to get the job done. As highlighted by Jim Collins in his best-selling management book *'Good to Great',* **people** are not your greatest asset; the **right people** are.

5. Actively monitoring risks:

   - With most public sector agencies understanding risk management is now in effect a necessary element of departmental approaches, there is a risk that it is treated as a 'tick the box' exercise. The very strong message here is that those responsible for developing policies or implementing programs or projects need to treat the exercise seriously, and ensure risk mitigation measures feed into the design and/or implementation strategies. In this context Defence now highlights publicly 'projects of concern' to ensure that the organisation/industry appreciates the elevated project risks. Recent events, globally and locally, also led the Financial Times to suggest that it pays to think hard about (nearly) unthinkable risks.

6. Modifying, or killing, projects that aren't performing.

- Some risks require more decisive action that monitoring. Such actions range from redesign through to killing programs or projects. In our work, we have seen projects that were killed, others that should have been a lot earlier.

If there is a central message here, it is about the importance of integrating risk management into all elements of organisational planning and execution. It is not about eliminating risk as that is impossible. The objective is very much about understanding risks, managing them and informing key stakeholders about them and the associated mitigation strategies.

As organisations grapple with the best way to enhance their focus on risk, I was interested to read the report of the Walker Review[17] of corporate governance in UK banks and other financial industry entities (BOFI).

One potential framework issue raised by Walker concerned the need for enhanced governance of risk, and he has suggested that best practice in a bank or life assurance company is for the establishment of a board risk committee separate from the audit committee.[18] His argument is that in practice the audit committee has clear responsibility for oversight and reporting to the board on the financial accounts and adoption of appropriate accounting policies, internal control, compliance and other matters. This vital responsibility is essentially, though not exclusively, backward looking.

Closely related, but separate, responsibilities are the critically important oversight of current risk in real-time in the sense of approving and monitoring appropriate limits on exposures and concentrations; and determination by the board of its risk tolerance and risk appetite through the cycle in the context of future strategy. This is largely a forward-looking focus designed to address past failures in risk assessments by boards.

Walker's essential point was that a clear differentiation is needed in ensuring that appropriate and separate focus is given to backward and forward-looking risk factors. Further, in support of board-level risk governance, a BOFI board should be served by a Chief Risk Officer who should participate in the risk input and oversight process at the highest level and should have a status of total independence from individual business units.

The value of such a committee with a focus on current risk and future strategy for some public sector entities is well worth consideration. For departments, in particular, it would be best orientated to the risks and uncertainties in, and options for, delivering government outcomes that are the administrative responsibility of the portfolio. Such an approach recognises earlier comments to the effect that the consequences of poor choices and poor program implementation in the public sector are severe, and deserve high level and focused consideration.

While I have highlighted factors that are important to effective risk management, it is also important to acknowledge that many program managers in many organisations are ensuring the delivery of services, and new approaches to the delivery of services, every day.

We have come a long way but there is no place for complacency. More will be expected of the APS.

With an eye to the future, the ANAO recently issued a Better Practice Guide (BPG) on Innovation in the Public Sector.[19]

The BPG aims to assist understanding of the pre-conditions and processes that underpin public sector innovation, and to offer practical help to public service practitioners.

The BPG's focus is on the culture and practices that can be adopted to encourage and facilitate innovation in the public sector. It sets out a measured approach to the public sector innovation process.

Innovation inevitably involves a degree of risk because it changes the *status quo* or contributes towards an alternative future. As such, an appetite for risk and risk management is essential; and risk avoidance is an impediment to innovation. This was a key message to get out; and a key message for the ANAO to acknowledge.

All public sector organisations will be required to be innovative to achieve the improvements in services and outcomes expected by stakeholders, and to make the productivity increases anticipated in budget funding models for agencies. Stakeholder engagement will be important to success here.

Where innovations do not reach their objectives, or mistakes are made, it is crucial to learn from the experience in a positive way. Learning from sub-optimal outcomes and mistakes is as important as celebrating success in reinforcing an innovation culture.

It is important that those of us with leadership responsibilities articulate the aspirations and strategic directions of our organisations, and make sure appropriate attention and resources are directed to medium and longer term issues where innovation is likely to be critical to success.

When risk management standards provide a sound basis for risk management, yet we still have failures in managing risks successfully, we need to look further afield to understand the organisational issues and dynamics that create sub-optimal outcomes, and learn from this.

III Concluding comments

The most successful organisations recognise that risk is part of doing business – it is all around - and that it can be managed with positive results. Those with leadership responsibilities have an important role in ensuring an organisation's approach to risk management is integrated into all elements of organisational planning and execution and sufficient resources are directed to risk intelligence.

We are well served with overarching guidance on risk management provided by the risk management standards which provide a framework against which the probability and consequences of an action can be mapped to derive a risk rating both before and after mitigation measures are put in place.

However, as I have noted earlier in this paper, having a robust risk management construct and standard in place is not enough — it comes down to successful implementation.

In the public sector we generally have well-established risk management frameworks, which are applied from the enterprise to project level. The implementation of risk management procedures is a necessary part of decision-making processes and should be 'fit for purpose'. That is, the degree of oversight and specific mitigation activities should be commensurate with the value, complexity and sensitivity associated with the delivery of particular programs and policy initiatives. On the basis of the work of the ANAO, the soft spots in public sector risk management relate to the understanding of the significance of identified risks, the appropriateness of the related risk management strategies, and the adequacy of on-going monitoring arrangements. Executive management has an important role in ensuring a focus on these key issues.

As for developments in risk management, I found the concept of the organisational risk radar, referred to earlier, a useful way to logically structure the consideration of risks. The main message here is that organisations can generally absorb strategies and approaches into their culture if they are logically presented and appropriately reinforced by agency practices and senior leadership. The concept of a board risk management committee separate from the audit committee may also be beneficial in some large public sector agencies.

Thank you for the opportunity to share these perspectives with you.

Notes

[1] The title of my presentation is drawn from the movie *'Love Actually'* where Bill Nighy's character, Billy Mac, changes the title and lyrics of The Troggs 1967 classic hit '*Love Is All Around*' to '*Christmas Is All Around' – 'I can feel it in my fingers, I can feel it in my toes'*.

[2] Booz & Company ' *Bringing Back Best practices in Risk Management Banks Three lines of defense'*, found at www.booz.com

[3] Murray, David, 'Challenges For APEC In The Post Global Financial Crisis Era', Australian APEC Study Centre, RMIT, 1 December 2009

[4] Roylett, Brian, *Lack of positive RM contributes to GFC,* Risk Professional, May 2009, p1

[5] McPhee, Ian 2007. *Project Management – some reflections on the management of projects in the Australian Public Sector*. Presentation to the Australian Institute of Project Management, Hobart, 9 October, p.2

[6] See Deloach, James W, Partner, Arthur Anderson, 2000. Executive Briefing: *An Executive Summary of Enterprise-wide Risk Management. Strategies for linking risk and opportunity*

[7] Ibid, p. 11

[8] Deloitte, Global Risk Management Survey: Sixth Edition Risk management in the Spot Light, 2009, found at www.deloitte.com

[9] Ernst & Young, Australia 2010. *The Ernst & Young business risk Report 2010 – The top 10 risks for global business*. Found at www.ey.com/au

[10] Mark Fenton-Jones 2010. Australian Financial Review. 'Professional Services' *Advisers thrive on risk issues*. 30 July. p.47

[11] Houchell Gavin. Reported in a recent newspaper article by Sam McKeith. *Risk managers 'the new black' as hiring soars*.

[11] Matthews, Mark, *Fostering creativity and innovation in cooperative federalism – the uncertainty and risk dimensions; Critical Reflections on Australian Public Policy* – selected essays. Edited by John Wanna. Grahame Cook, PSM, Director of Grahame Cook Consulting Pty Ltd and Mark Matthews worked with the ANAO in developing an Innovation Better Practice Guide, *Innovation in the Public Sector: Enabling Better Performance, Driving New Directions*

[13] The Standish Group International CHAOS Ten Success factors 2009

[14] The 2009 Victorian Bushfires Royal Commission final report, July 2010, p.79

[15] Ibid, p.80

[16] Ibid, p.83

[17] Walker, Sir David, *A Review of Corporate Governance in UK Banks and Other Financial industry entities,* HM Treasury, 16 July 2009.

[18] Ibid., p81

[18] *"Innovation in the Public Sector: Enabling Better Performance, Driving New Directions"* ANAO Better Practice Guide, December 2009