AUSTRALIAN NATIONAL AUDIT OFFICE

Heads of Cultural Organisations Meeting

Risk Management

15 December 2005

Ian McPhee
Auditor-General for Australia

Australian National Audit Office

HEADS OF CULTURAL ORGANISATIONS MEETING
Thursday 15 December 2005

'Risk Management'

Speaking Notes of Ian McPhee, Auditor-General for Australia

Thanks for the invitation to address the group today on the topic of Risk Management.

- I was reflecting last night on what I would be able to tell the heads of DCITA agencies about risk management;

  - you wouldn't be in your positions without a good grasp of risk management, although, as I read in the papers, there are always new challenges or old challenges with new risk ratings;

  - the main point, though, is that organisations require a disciplined approach to risk management compared to the more intuitive approach adopted in years past.

- I thought I should check the web for the latest on *'risk management'*
  - there were 242 million hits in 0.2 seconds:
  - so much information, so little time.

- To narrow the search, and given the time of year, I combined 'risk management' with 'Santa Claus'
  - still 45,600 hits!
  - even a joke to share with you from the Insurance Professionals website: *"A **smart insurance company executive** and an **honest broker** were seen walking down the street with Santa Claus. They all spotted a $50 bill lying right in the middle of the side walk. **Who picked it up?** Santa did…… a smart insurance executive and an honest broker are figments of your imagination!"*[1].

[1] www.rmis.rmfamily.com

Risk can be defined simply as:

'***Uncertainty in achieving organisation objectives'***[2]**.**

- Risk management is now a readily recognised element of the management discipline; its application though is not always as recognisable;
  - against this background, it is useful to have some points of reference to guide its application.

- Anthony Atkinson and Alan Webb of the University of Waterloo, Ontario, make the point that the fundamental nature and consequences of risk apply equally to for-profit and not-for-profit organisations:
  - In for-profit organisations, risk is usually formalised as the uncertainty of financial returns;
  - In not-for-profit organisations, risk is usually formalised as uncertainty in achieving the organisation's stated quality objectives.

- Atkinson and Webb also state that:
  "the primary roles of risk management are to identify the appropriate risk return trade off, implement processes and courses of action that reflect the chosen level of risk, monitor processes to determine the actual level of risk, and take appropriate courses of action when actual risk levels exceed planned risk levels."

- At a conceptual level, there are three major contributors to organisation risk:

  - **Strategic risk**: defined as the concern that major strategic alternatives may be ill-advised given the organisation's internal and external circumstances;
  - **Environmental risk**: covering macro-environmental factors, competitive factors and market factors; and
  - **Operational risk**: covering compliance risk and process risk.

[2] Atkinson, Anthony A and Webb, Alan, *A Directors Guide to Risk and its Management*, International Federation of Accountants Articles of Merit Award Program for Distinguished Contribution to Management Accounting, August 2005, p. 26.

- What I like about Atkinson & Webb's model is that it clearly states the role of risk management and the contributors to organisation risk (and how risk management should be self regulating).

- Those charged with governance are expected to act in the interests of their primary stakeholders and identify, evaluate and respond to the entity's risks — encompassing risks relating to strategy and programme or business operations, including risks related to compliance with laws and regulations.

- Stakeholders expect those charged with governance of an entity to manage strategic and environmental risks and to put controls in place to deal with such risks. Managers at all levels can also be expected to manage strategic, environmental and operational risks so that, if 'controls' are working properly, the **net risk** rather than the gross or inherent risk is managed. *(Managing risk is not someone else's responsibility).*

- A survey of public and private company directors in the United States, suggests that boards of directors consider risk management one of their most important responsibilities. However results from the same survey show that:

    - Less than 30% of directors believe their boards are highly effective in managing risk;

    - Similarly, 36% of directors who responded to a 2002 survey conducted by McKinsey & Company indicated they did not fully understand the major risks their organisations face, and 42% did not understand fully which elements of the business created the most value for shareholders.[3]

- In corporate Australia, the importance of recognising and managing risk is acknowledged. Indeed, Principle 7 of the ASX Principles of Good Corporate Governance and Best Practice Recommendations mandates the requirement to establish 'a sound system of risk oversight and management and internal control' by:
    - identifying, assessing, monitoring and managing risk;
    - as well as informing investors of material changes to an organisation's risk profile.

[3] Atkinson, Anthony A and Webb, Alan, *A Directors Guide to Risk and its Management*, p26

- Risk management has general application, but in industries where fiduciary responsibility is critical, legislation commonly requires the specific application of risk management procedures. For example, APRA's Prudential Standards requires that a *'general insurer has systems for identifying, assessing, mitigating and monitoring the risks that may affect the ability of the insurer to meet its obligations to policy holders. These systems, together with the structures, processes and people supporting them, are referred to as the insurers risk management framework."*[4]

- The APRA requirements are not just stated as a high level objective, but, inter alia, go on to require:

  - a documented Risk Management Strategy including sound risk management policies and procedures, and clearly defined managerial responsibilities and controls;

  - periodic internal audits of the effectiveness of the risk management framework must be undertaken by the insurer;

  - the submission of a Risk Management Declaration by insurers to APRA on an annual basis.[5]

- More broadly, APRA, as part of its supervisory approach, looks in detail at operational risk and how it is managed in its approach to risk-rating regulated institutions. APRA expects each institution to develop its own framework to identify, measure and manage operational risk that is relevant to its specific circumstances and is in line with the risk appetite set for the institution by its board.

- I am not suggesting that APS agencies should replicate risk management practices applied by financial institutions but we can benefit from the approach adopted here.

  - as heads of public sector agencies we may not have the same fiduciary responsibilities as financial institutions, but given our responsibility to manage *'public funds in pursuit of public*

---

[4] John F Laker, Chairman, Australian Prudential Regulation Authority *'Operational Risk Management: A Prudential Perspective.'* Instol/AFOA 2nd Annual Conference 2005, Sydney, 25 August 2005.

[5] APRA: Draft Prudential Standards – General Insurance Risk & Financial Management. GPS 220 Risk Management – www.apra.gov.au

benefit' (Peter Shergold) we do have obligations to actively manage risks to effective performance.

- We in the public sector have traditionally been seen to adopt a more risk-averse approach to management generally.

- Some of this, no doubt, arises due to the importance of the legal framework which guides public administration, and the fact the public moneys need to be managed with due care.

- Parliamentary Committees, in my experience, have generally been open to the explicit application of risk management by public sector entities – it is when entities are not able to adequately explain their approach to risk management that issues arise from time to time.

- In its report on Contract Management in the APS, the Joint Committee of Public Accounts and Audit, made the point that risk management is an integral part of good management practice and where risks are managed poorly there can be significant costs for agencies.

- However the Committee also noted that a key benefit of risk management is the optimisation of opportunities and it must be managed proactively rather that reactively.

- The debate about whether a more risk averse approach is being adopted is not one that relates only to the public or financial sectors.

- Some commentators believe that in our current climate, a more risk-averse attitude is being generated with the increasing emphasis on compliance due to the responses from the corporate regulators around the world to the well-publicised recent spate of corporate collapses.

- However, the way I see it is that compliance with laws and standards is now arguably more important to stakeholders (including investors) and risk assessments need to be recalibrated in this light. That is, it is not a matter of being risk averse but rather a recognition that the consequences of non-compliance can be more severe that some risks assessments have assumed.

- For some years now, Governments at both the federal and state levels have been increasingly focused on achieving a better performing public sector.

- A major imperative has been a drive for greater efficiencies and effectiveness through providing services that are less costly, more tailored, better directed, and of higher quality to their customers or citizens.

- The boundaries between the public and private sectors are becoming more porous; and policies that demand whole-of-government approaches are becoming more common.

Whole of Government Risk

- Public sector organisations must not only manage their own risks but also the risks that come with joined-up government and inter-agency partnerships;

  - managing such complexity involves managing increasingly complex risks.

- A paper titled *'Risk: Improving government's capability to handle risk and uncertainty'* developed by the UK's Strategy Unit puts the proposition in this way:

  'Governments have always had a critical role in protecting their citizens from risks. But handling risk has become more central to the working of government in recent years. The key factors include: addressing difficulties in handling risks to the public; recognition of the importance of early risk identification in policy development; risk management in programmes and projects; and complex issues of risk transfer to and from the private sector'.

- The paper sees risk in the public sector expanding to embrace: direct threats (terrorism); safety issues (health, transport); environmental (climate change); risks to delivery of a challenging public service agenda; transfer of risk associated with PPPs and PFIs; and the risks of damage to the government's reputation in the eyes of the stakeholders and the public and the harm this can do to its ability to deliver its program.

- Taken together, these concerns have forced governments to reappraise how they manage risks in all its forms. And we have seen this occur in Australia.

- The Strategy Unit's paper makes the strong point that governments also have clear roles in managing risk. Where individuals or businesses impose risks on others, government's role is mainly as regulator. Where risks cannot be attributed to any specific individual or body, governments may take on a stewardship role to provide protection or mitigate the consequences. In relation to their own business, including provision of services to citizens, governments are responsible for the identification and management of risks.

- Governments need to make judgements in as open a way as possible about the nature of risk and how responsibilities should be allocated, recognising that there will always be some unavoidable uncertainty.

- When implementing whole-of-government programs, the ANAO in a recent audit report, highlighted the importance of leadership (ie appointing a lead agency) to integrate and link activities such as risk management and performance assessment of the implementation process, rather than relying solely on specific agencies' performance indicators.

- There is now a recognition by agencies that an effective risk management strategy and control environment must be in place and that they must continually refine their risk management requirements to actively manage their changing risk profiles – this is no longer discretionary.

- An added complexity is the quickening pace of public administration, including policy development and implementation, which means that not all policy details may be settled before a policy is announced nor are all implementation details bedded down before implementation commences.

- This requires an agile approach to risk management with experienced and senior managers oversighting the process. Indeed, those key judgements and risk assessments that are critical to the successful delivery of a program or policy require intensive scrutiny or to use the vernacular — the 'blow torch' applied to them.

- Against this backdrop, the thrust of my presentation today is that those charged with governance of an organisation, and managers, must be concerned with the identification, evaluation and treatment of an organisation's risks — what I call *'organisational self-awareness'*.

- While public sector chief executives are commonly required to deal with an array of policy, program and organisational issues, it is also important that ongoing attention is given to measures to reinforce good governance and effective administration.

- Risks encompass those relating to strategy, operations, reputation as well as those relating to compliance with laws and regulations and financial reporting.

- An enterprise-wide risk approach (ERM) is increasingly seen as the preferred approach to risk management. ERM calls for high-level oversight of a company's entire risk portfolio rather than for many overseers managing specific risks – the so-called silo approach.

- Sir John Bourn, my counterpart in the UK, identified five key aspects of risk management which, if applied more widely, could contribute to better public services and increased efficiency, they are:

  - *Sufficient time, resource, and top level commitment needs to be devoted to handling risks;* (the toughest of all)
  - *Responsibility and accountability for risks need to be clear and subject to scrutiny and robust challenge;*
  - *Judgements about risks need to be based on reliable, timely and up to date information;*
  - *Risk management needs to be applied throughout departments' delivery networks;*
  - *Departments need to continue to develop their understanding of the common risks they share and work together to manage them.* [6]

[6] Bourn, Sir John, 2004, UK National Audit Office Press Notice: *Managing Risks to Improve Public Service*, 22 October, found at www.nao.org.uk

Risk Themes arising from ANAO Audit Reports

- ANAO audit reports emphasise the point that the management of risks is an integral part of the prudent administration of programs involving the expenditure of public funds.

- While good progress has been made in putting the machinery of risk management in place, there is still some distance to go before we can say that all public sector organisations have made effective risk management a central element of their day-to-day general management approach.

- APS entities generally need to do more on 'following through' on implementation and to be more proactive in managing risk by ensuring risks controls and treatments are in place across the organisation. Also, a better understanding of strengths and weaknesses is required. *(Organisational self-awareness)*

- The ability of agencies to capably manage risk can result in better delivery of government services through: improved efficiency (using a risk-based approach to organisational procedures/service delivery mechanisms); more reliable decision-making; and supporting innovation.

- Recent Audit reports have emphasised some common areas of administration where the greater application of risk management is likely to have achieved a better result, including in relation to:

  - project management;
  - contract management;
  - IT systems development and implementation;
  - performance measurement; and
  - business continuity management

Concluding Remarks

- I will draw my comments together by observing that risk management processes are increasingly well understood across the public sector, but the existence of the frameworks, and knowledge of the associated elements and processes, do not guarantee the proper treatment of risks across an organisation.

- To ensure that organisational objectives are being met, and priorities are being addressed in the manner agreed, an organisation-wide view of risks and controls is necessary.

- Such a view will reflect the culture, or 'tone', that has been set for the organisation by its leadership within its governance framework, based on a strong values/ethical commitment.

  - never underestimate the influence a CEO can have in this area.

- Having said that, risk management is everyone's responsibility. Senior managers should closely review critical risks and treatments.

- Organisations should recognise their strengths and weaknesses and particularly recognise the need to compensate for weaknesses. This organisational self-awareness is an important ingredient in effective governance and organisational performance.

15/12/05