AUSTRALIAN NATIONAL AUDIT OFFICE

Australian Institute of Company Directors, in conjunction with the Institute of Internal Auditors Australia

Public Sector Governance and Risk Forum

Risk and Risk Management in the Public Sector

Thursday 1 September 2005

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

Ian McPhee
Auditor-General for Australia

Australian National Audit Office

Risk and Risk Management in the Public Sector

I thank the Institutes for their invitation to speak at the 2005 Public Sector Governance & Risk Forum - I welcome this opportunity to share some insights and experiences relating to public sector governance and risk.

Introductory remarks

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:

> *'Risk is uncertainty in achieving organisation objectives.'*[1]

Anthony Atkinson and Alan Webb [2] 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 [3] 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**: 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.[4]

The identification and management of risk is an integral part of a sound management and governance framework in both the private and public sectors. 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, as well as risks related to compliance with laws, regulations and financial reporting. 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. That is, managing risk is not someone else's responsibility any more – responsibility resides at all levels in an organisation.

The key point here is that entities should adopt a risk-based approach to strategy and internal control, and assessments of their effectiveness. In other words, entities should mitigate the gross or inherent risk involved in a business activity and determine the net risk to be borne by the entity. Such an approach needs to be incorporated into the strategic, governance and management processes of the entity and should encompass the wider aspects of internal control, not just those related to financial reporting. [5]

A survey of public and private company directors by the National Association of Corporate 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.[6]

In corporate Australia, the importance of recognising and managing risk is acknowledged. Indeed, Principle 7 of the ASX Corporate Governance Council's *Principles of Good Corporate Governance and Best Practice Recommendations* (issued in March 2003) 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. The supporting recommendations suggest that the chief executive officer and the chief financial officer should state in writing to the board that the integrity of financial statements is founded on a sound system of risk management and internal compliance and control, and that the company's risk management and internal compliance and control system is operating efficiently and effectively in all material respects.

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 that 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 [7], the Joint Committee of Public Accounts and Audit makes 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 must be managed proactively rather that reactively.

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. 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.[8] When implementing whole-of-government programs, the ANAO in a recent audit report[9], 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.

The Secretary of PM&C, Dr Shergold, reinforces the point that the Australian Public Service (APS) has become increasingly complex with a plethora of Commonwealth agencies existing alongside the Departments of State with their governance arrangements varying markedly. Agencies enjoy varying degrees of independence and the array of 'boards', wielding different levels of responsibility, makes the lines of authority between the Minister, Secretary and agency head more difficult. [10] He makes the point that governance, in the public sector, presents significant challenges over and above the private sector, indeed '*Public sector governance is marked by the fact that it manages public funds in pursuit of public benefit*'. [11] It involves an understanding of the nuances of the relationship between a Minister and a Secretary, between ministerial advisers and public servants and between an elected Executive government and an appointed Executive service. In the words of Lynelle Briggs, the Public Service Commissioner:

> *A key role for an agency head is to devise an approach to governance that enables the agency to adhere to its corporate goals in a manner consistent with applicable legal and policy obligations.* [12]

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. The extent to which public sector entities have embraced enterprise risk management illustrates the maturity of risk management in the Australian public sector.[13] The ANAO has played its part in shaping a more contemporary risk management approach through our Better Practice Guides, and importantly, highlighting risk management issues in our financial statement and performance audits.

I also need to emphasise that risk is a strategic issue which needs to be aligned to strategic objectives, corporate governance arrangements, and integrated with business planning and reporting cycles. Put another way, risk management needs to be integrated into strategy development as well as business planning to achieve organisational goals and optimise performance. Put succinctly, risk should be treated as a strategic issue so that:

- planned business outcomes, outputs and activities do not expose the organisation to unacceptable levels of risk;

- use of resources is consistent with organisational priorities; and
- the risk management strategies are integrated with the management actions of staff at all levels in the organisation, including recognition that all staff have a responsibility to manage risks. [14]

This approach provides the appropriate assurance to Government and other stakeholders that the agency has a formal, systematic and pro-active approach to the identification, management and monitoring of risk. [15] This has, perhaps, been the most significant challenge for public sector entities and is likely to continue to be so.

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.

Let me now turn to the current state of play of Risk Management, primarily in the public sector, and provide some insights into lessons learnt from the ANAO's audits of public sector entities.

The Current State of Play

As corporate governance receives increasing attention—I have heard it referred to as an *'unrelenting tide'* [16]— it is becoming almost a given that effective risk management, as a corner stone of good corporate governance, results in better service delivery, more efficient use of resources, and better project management, as well as helping to minimise waste, fraud and poor value-for-money decision-making.

Warren Gillian (Deputy Director of the Australian Risk Management Unit at Monash University) in discussing the role risk management plays in improving performance and achieving effective governance

describes risk as a *'whole of organisation activity'* with risk management needing to be integrated into strategy development as well as business planning. He also stressed that risk management needs to be understood at the top levels of an organisation. [17]

Increasingly, all organisations, both private and public sector, are being asked to show evidence of a systematic approach to the identification, analysis, assessment, treatment, and ongoing monitoring and communication of risk.

Increasingly an enterprise-wide risk approach (ERM) is 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. [18] The contrast between the more tradition risk management approaches and ERM is well illustrated in a recent article published by the International Federation of Accountants in its *Articles of Merit Award Program*. [19]

Traditional RM vs ERM: Essential Differences

Traditional risk management	**ERM**
Risk as individual hazards	Risk in the context of business strategy
Risk identification and assessment	Risk portfolio development
Focus on discrete risks	Focus on critical risks
Risk mitigation	Risk optimisation
Risk limits	Risk strategy
Risk with no owners	Defined risk responsibilities
Haphazard risk quantification	
'Risk is not my responsibility'	'Risk is everyone business'

Source: KPMG as cited in Enterprising Views of Risk Management [20]

Despite its many complexities, risk management is essentially a management tool to help ensure that an organisation has the right controls in place to protect itself against adverse results.[21] Notwithstanding the general recognition that good corporate

governance steers management towards the better risk decisions—that is, well informed risk decisions as opposed to risk avoidance—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 than some risks assessments have assumed.

I mentioned earlier the tension created by the public sector culture, vis-à-vis the need to operate using modern risk management principles. This is now being recognised within the public sector and increasingly by our Parliamentarians, particularly the Joint Committee of Public Accounts and Audit.[22] This point was also highlighted by the United Kingdom's Committee of Public Accounts with its observation that:

> *'Innovation to improve public service entails risk. We are rightly critical where risks are ignored, for example where major IT projects are poorly specified and managed; but we give due credit where risks are carefully identified, evaluated and managed recognising that good management reduces but does not eliminate the possibility of adverse outcomes'.* [23]

That said however, in the public sector, for those projects where formal assessments should be in place, much of the approach to risk management continues to be intuitive rather than as a result of a strict application of the risk management standard (4360:2004 Standards Association of Australia). However the good news is that there is a greater appreciation within agencies of the need to adopt an effective risk management approach. And, while it is easy to talk about a systematic approach to risk identification, risk assessment, prioritisation and risk treatment, the substantive issue is how are the various risks confronting organisations actually being addressed in ways that provide assurance (internally and externally) about performance and the outcomes (results) achieved. Implementation continues to be the real problem.

Applying the principles and practices is no guarantee of success and, as always, the proof of the pudding is in the eating. So, can we draw some general conclusions about how well risk management has been implemented?

One well-placed observer, COSO's new chair Larry Rittenberg, seems to think that US corporations (at least) have a way to go. In responding to a question recently on the implementation of ERM he made the point that organisations are holding up their hands saying '*We understand that we have to do a better job of dealing with risk*'. He believes that too many organisations have failed because they did not have comprehensive risk programs in place and he expects that the implementation of ERM will come gradually across organisations. He believes that it has already started in pockets of many organisations and will spread to other areas as management finds it to be a useful way of analysing strategy and ensuring that the organisation has adequate controls — boards and managers are like other human beings – they react to pressure points.[24]

Closer to home, research commissioned by Hewlett Packard and Mallesons Stephen Jaques showed that Australian firms are exposed due to a lack of alignment of corporate and IT governance. The research indicates that in a significant number of organisations corporate governance and IT governance continued to be treated as separate strategies rather than as one with a single goal. Despite IT's criticality to most areas of business, IT strategies are not being treated as an integral part of overall business strategy. [25]

For the internal auditors among us, I read with interest the comments of the Institute of Internal Auditors' (IIA) new chairman of the board, Thomas Warga, where he observed that *'in an increasing number of our organisations, there is a convergence of risk management, internal control, and governance, and pulling this altogether is where the internal auditor can make a contribution'*. [26] This fits well with the basic requirement for the internal audit function, as set out in the new Internal Auditors Australia (IAA) standards, to monitor and evaluate the effectiveness of an organisation's risk management and control systems. Standard 2110 of the International Standards for the Professional Practice of Internal Audit, for example, states that the internal audit activity should help the organisation manage risk by identifying and evaluating significant exposures to risk and contributing to the improvement of risk management and control systems. [27]

From a public sector perspective I offer this initial observation taken from a recent ANAO audit report:

> *'Entities need to continue to build risk awareness; strengthen business practices and systems of authorisation…as part of the development of performance measurement frameworks'*;[28] and *'Entities generally acknowledged that enhancements were necessary in increased risk awareness assessment and better management, including the use of performance management*

> *tools such as data metrics to monitor trends in risk and its treatment'.* [29]

Sir John Bourn, my counterpart in the UK, made this observation which I believe resonates here as well:

> *'Today's public service delivery environment constantly presents new risks to the provision of public services, and robust risk management can help departments respond effectively. Just as importantly it opens up opportunities to develop innovative policies and delivery mechanisms. … I have identified a number of ways in which departments can make further progress in developing cultures that place active, explicit and systematic risk management at the heart of their business so that decisions are routinely based around accurate and well informed judgements about risk. It is critical that departments continue to build on the momentum achieved so far in developing their risk management…'*[30]

Sir John went on to identify 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;*
- *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.* [31]

Before I move on to distil some risk management themes arising from some of the ANAO's recent audit reports, I want to touch on two topical issues in public administration today. The first relates to the greater focus on whole-of-government approaches to public administration, the second is the importance of reputational risk and the damage that can be done to an entity's reputation in the eyes the public and the harm this can do to its ability to deliver its programs.

Whole of Government Risk

As already canvassed, the boundaries of risk management have expanded from the previous 'silo' approach to an agency (or enterprise)-wide risk paradigm — now, whole-of-government issues are coming into play. A paper titled *'Risk: Improving government's capability to handle risk and uncertainty'*[32] developed by the UK's Strategy Unit puts the proposition thus:

> *'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'.* [33]

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.[34] Taken together, these concerns have forced governments to reappraise how they manage risks in all its forms. The ANAO has also commented on the whole of government impact in at least one recent audit report:

> *'The ANAO considers that a more consistent approach to risk management is required to appropriately address program risks. This would require more systematic risk management planning by DIMIA, consistent with its approach to agency-wide risk plans, as a means of ensuring consideration of risks from both an enterprise-wide and a whole-of-government perspective'.* [35]

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. [36]

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.

Reputation risk

A recent edition of the Australasian Risk Management Newsletter noted that reputation risk can be a major risk for all commercial organisations regardless of size, as well as not-for-profit and government bodies[37]. The article observed that little attention is paid to this risk by management boards except when an incident arises that negatively impacts on an organisation's reputation. The same might be said about some government bodies. The article makes two key points—reputation risk should be managed as part of an organisation's normal risk management process, and, second, the risk should be totally integrated with the operational risk processes[38].

Reputation damage is possibly the most misunderstood and ill-managed of an organisation's risk management activities and no amount of crisis management can usually repair the damage—as was the case with Arthur Andersen, where clients and staff were looking to leave before any allegations were proven. [39] Another example, closer to home, is public criticism levelled at the Red Cross over how it spent funds raised for the 2003 Bali bombing victims. Although an independent audit cleared the Red Cross of any wrongdoing, the charity's reputation was affected when the audit found that it had not spent the percentage of funds raised on the bombing victims as it had promised. *'Managing an organisation's "good name" is a core purpose of all boards, because reputation management is fundamental to ensuring the financial viability of an enterprise'*. [40]

Let me now move on to some insights from our audit reports.

Risk Themes arising from ANAO Audit Reports

The management of risks is an integral part of the prudent administration of programs involving the expenditure of public funds. It should include a framework for cost effectively treating, or minimising, the risks to a program such as the realisation of the program's objectives or value for money outcomes. It is both an accountability and a management tool and should be part of the initial program design to assist Ministers and agencies in their decision-making.[41]

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.

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.[42] As the ANAO observed recently:

> *'Risk management is important because it allows the identification, assessment and treatment of risks that may, if untreated, prevent an agency achieving its objectives or not achieving them to the level required'.* [43]

Looking at the risk management comments in a selection of recent ANAO audit reports we can identify some common themes. I stress that the following is a selection only of the more contemporary issues.

Theme 1 — Information Technology

The continuing technology developments and advancements, together with the ongoing implementation of these technologies by entities has introduced a new range of risk management issues and concerns. It also has an impact on IT governance and the reliability of an entity's IT processes. A particular issue is the increasing demand to provide more integrated and interactive information and services, in order to improve the management and delivery of government programs. This has continued the move toward e-Government to provide more responsive, comprehensive and integrated government operations and service delivery.[44]

The management of IT related risk is a key component of corporate governance. Effective IT governance is integral to the success of overall governance by ensuring efficient and effective planning, management and operation of IT processes, IT resources and information. IT governance provides the structure to link and align technology to entity strategies and objectives.

Entities' IT processes and systems will need to transform to respond to new technologies and to ensure that systems are compatible and integrated, both internally and externally. Each entity's management

of systems development will need to plan for future compatibility, interconnectivity and maintenance. Change management processes and procedures will also need to adapt to ensure the reliability and integrity of systems, and the information they process, is maintained in a systematic and controlled manner.

As a consequence of the continued move toward e-Government and the adoption of new technologies for interconnection and interoperability of systems, information security management will become an even more critical issue. As the implementation of new technologies transform the Australian Government, service delivery, contract management, configuration and storage management, as well as business continuity management will also become more important issues to be actively managed.

Looking at the development of large scale IT systems, not all APS agencies have a good track record. It seems that we don't take the lessons learnt to heart as evidenced by two of our very recent audit reports on two ambitious IT projects — The Edge Project [45] (Family & Community Services and Centrelink) and PMKeyS Project [46] (Defence).

The Edge Project [47]

To set the scene, Edge was a joint project between the Australian Government Department of Family and Community Services (FaCS) and Centrelink to develop an expert system for the Family Assistance Office (FAO). Edge was a processing application, for the administration of claims and payments for people applying for entitlement to family-related payments. At the commencement of the project, FaCS was the principal policy formulating and advising body in the portfolio. Centrelink was the service delivery agency in the portfolio, delivering a range of Commonwealth services, such as pensions, benefits and allowances to the Australian community.

Four things characterise this project:

1. The business case recognised that implementing a large expert system of Centrelink's scale was a high-risk project.
2. Payments made by Centrelink were subject to increasingly complex and frequently changing rules.
3. There were tensions between FaCS and Centrelink during the project — FaCS and Centrelink were never able to agree a MOU for the project.
4. Changes to the Families program undercut the original raison d'etre of the project. Indeed, an independent review in 2002 recommended the termination of the project commenting that Edge in its planned form was no longer properly aligned with the business needs of the Families program; the operation of

> Edge in parallel with the ISIS (the mainframe system) was unsustainable; changes to the Families program meant Edge could have only limited effect on a key driver—improvement in accuracy; and the level of anticipated benefits were unlikely to be realised, leading to a negative return on investment.

In looking at Edge the ANAO concluded that the governance of the project was not as effective as it should have been, in that:

- predictions given to the agencies' Executives of the number of customers that could be processed through the system were optimistic, and never met;
- advice that a high level of claims processed through ISIS could have been avoided using Edge, was optimistic and potentially misleading;
- the FaCS governance committee with responsibility for IT was not involved in the project;
- it was not clear that the FaCS Executive Board and Centrelink Board of Management were informed of the lack of progress on agreeing the MOU ;
- the joint FaCS–Centrelink Steering Committee did not meet during the latter two years of the project;
- responsibility for the project was split between the two agencies, with no Senior Responsible Owner identified;
- an MOU between FaCS and Centrelink was never agreed, and hence funding and savings were never agreed; and
- the project plan was not maintained, and there was no formal development methodology.

The PMKeyS Project [48]

PMKeyS was to become Defence's core management information system for personnel management for both civilian and military staff. The project was to encompass the full gambit from leave to training, career management and workforce planning—in other words an ambitious project. In commenting on Defence's financial statements for 2003-04, the ANAO was unable to express an opinion whether the statements were true and fair due in part to deficiencies in the PMKeyS system.

Looking at this project, it follows a not unfamiliar story: the project suffered extensive schedule slippage; major outcomes had not been delivered; projected savings of $100m per annum were not demonstrated (six months after the project was closed the system was yet to demonstrate a return on investment); the project exceeded budget costs by 150%. (there was not an effective control over project

costs and outcomes). Additionally, project approval was not in line with government requirements and the project was not managed as a strategic procurement activity, nor was it managed as a Major Capital Equipment project.

The lessons learnt from the PMKeyS include:

- The need for project approval processes for IT systems to comply with Government and departmental requirements to ensure improved project governance arrangements;
- Defence incurred significant project and infrastructure related expenditure in excess of the original funding allocation. To improve relative project cost and schedule outcomes, future management information system projects should be based on realistic estimates of project costs and system infrastructure requirements that have been subject to close analysis and review, prior to project approval;
- The need for a structured process of periodic management review following the awarding of contracts to provide additional assurance on schedule, cost and performance outcomes being;
- Project management business processes should accord with sound management practice for contractual and financial management, and for the retention of appropriate records, to ensure legislative compliance and that project outcomes meet with end-user needs; and
- Meaningful and measurable key performance indicators should be implemented to assist Defence in the monitoring of the effectiveness of management information system remediation initiatives.

Theme 2 — Record-keeping

The issue of record-keeping is currently receiving quite a lot of what I would regard as 'deserved' attention, including comment in a recent financial statement audit report which made reference to the requirement to keep proper records,[49] and the need to improve the implementation of effective records management systems in the audit report on the management of selected Defence project offices. [50]

Records are necessary for us to function properly. In a relatively recent audit report, the ANAO noted the importance of record-keeping as '*a key component of any organisation's corporate governance and critical to its accountability and performance*'.[51] Among a number of recommendations for improvement in record-keeping practices, we suggested that:

> *'The risk assessments should also review record-keeping from an operational perspective so that organisation's record-keeping priorities do not pose any legislative or business risk to the organisation'.*[52]

Associated with these above risks is the growing importance of web sites as sources, and in some cases the only sources, of many organisational records. The risks of not properly capturing these in a record-keeping system is a new and growing concern. In a recent article *'Web Sites as Recordkeeping & Recordmaking Systems'* [53], Rick Barry makes the point that web sites produce official representations to the public and, while they make records, they do not keep records in ways that are consistent with sound record requirements.[54] That is, web sites are among the key organisational record-making systems that are not record-keeping systems—this places organisations at risk.

Clearly, the rapid uptake of e-business and e-government applications using Web publishing systems has outpaced the ability of many organisations to properly manage the records produced in these systems. Often this is accompanied with a lack of appreciation in the organisations that websites produce records. So long as this technology is used for business, and interacting with the public, the content and transactions on these sites constitute organisational records and therefore must be captured, preserved, and managed into a paper-based or electronic records system. [55]

Rick Barry makes the important point that, for most organisations, the integration of Web content and electronic records management is essential. Failure to do so puts the organisation at considerable legal, regulatory, and even ethical risk, and opens it up to alienation from its client and public base. Moreover, it robs the organisation of one of its vital assets—its corporate memory. [56] The volume of content, associated with significant business and/or legal risks, places attention on the need for a so-called 'content management system' which has to support 'a solid review and approval process that is enabled via an easy-to-administer workflow component' [57] It is suggested that the ready availability of high-quality and current education and training sends a clear message to all in the organisation that content management 'is a priority and a necessity'.[58]

Theme 3 — The need for more structured and proactive Risk Management

For this theme I have selected two audits which I believe draw out the issues quite well, the first from a regulator's perspective, the second relating to outsourcing and contract management.

Regulation of Non-prescription Medical Products [59]

The audit report makes the point that sound and structured risk management is central to performing a regulator's function as well as the assessment of risk being an important element in its operational procedures. For example, in the Therapeutic Goods Administration (TGA) case, risk considerations influence the setting of audit frequency and product testing.

The audit found that aspects of risk management for non-prescription medicines required better articulation and structure to support targeting and monitoring of risk treatments. The ANAO recommended that the Department review and enhance the TGA's risk management framework (for non-prescription medicinal products) with the revised framework being systematic, structured and integrated with the TGA's overall risk management strategies. In addition, resources need to be allocated to the various risk treatments, and to ensure new or targeted strategies are based upon structured risk assessments and their outcomes are evaluated for lessons learned for future management of compliance.[60]

Management of the Detention Centre Contracts [61]

This audit focused on whether the risks associated with contracting out detention services were identified, assessed and treated appropriately. The audit found that DIMIA's management of the program, together with the delivery of services under the contract and the prioritisation of tasks, was reactive rather than proactive. That is, it focused on risks that arose, rather than pursuing systematic risk analysis, evaluation, treatment and monitoring. The report made the point that a systematic approach to risk management, including the establishment of an appropriate and documented risk management strategy, should be an integral part of contract management. [62]

Although DIMIA acted appropriately to deal with program and other risks as they occurred, the majority of risks were managed in response to an incident or event. Clearly, it is better practice to put in place, preferably on an enterprise-wide basis, effective preventative action or at least action that minimises or ameliorates, an adverse risk event. This applies not just to financial risks but also, importantly, to

strategic and operational risks associated with delivery of the services.[63]

Additionally, the audit found that DIMIA had not developed treatment plans to reduce unacceptable risks. In particular, there was no mechanism for monitoring and reviewing the risk profile—for example, there was no provision to allocate responsibility between DIMIA and contractor to control new risks that emerged during the course of the contract. [64]

Theme 4 — Risk and Insurance

Despite the stimulus that initiatives such as the establishment of Comcover provided for sound management practices, the maturity of risk management and insurance practices across the five organisations examined as part of our Management of Risk and Insurance audit [65] (and of the 50 organisations surveyed) generally needed to be improved.

Overall, the ANAO concluded that general insurance frameworks and practices had the greatest potential to be improved, notwithstanding the training, education and consulting support provided by Comcover. Organisations audited had at least applied basic occupational health and safety (OHS) and workers' compensation frameworks and, in some cases, had sound frameworks and practices in place. The quality of risk management frameworks and practices tended to be better than for general insurance practices but were often not as sound, or as well supported, as OHS and workers' compensation frameworks. [66]

The level of maturity of the practices of these organisations varied significantly. A major factor that contributed to a lack of maturity in risk management practices was the dominance of management 'silos', which limited their ability to take an organisation-wide perspective. [67]

While Comcover provides guidance to its client organisations regarding risk profile, level of insurance and deductibles, the ANAO found that the cost of insurance and level of deductibles was generally not being considered by organisations in relation to their risk profile, nor to their incidents and claims experience. The audit also concluded that, based on the organisations audited, and in most cases the organisations surveyed, improvements are required in relation to:

- *better understanding and articulation of the links between risk and insurance;*
- *better utilising risk management in business planning;*
- *consistently applying the risk and insurance frameworks in a timely manner;*

- *improving record-keeping and reporting of risk management and insurance activities;*
- *reviewing risk and insurance practices and performance on a regular basis;*
- *better resourcing of risk management and general insurance activities; and, most importantly; and*
- *an improved level of promotion and participation in applying the risk management framework by senior management.* [68]

Recent audits and studies conducted by State Audit Offices and CPA Australia identify similar findings and opportunities for public sector organisations in Australia.[69]

Theme 5 — Defence Materiel Projects

The *Management of Selected Defence System Program Offices* [70] audit highlights differences in relative management process maturity between the four System Program Offices (SPOs) examined. The ANAO found that Tactical Fighter SPO provides an example of better program management practice, in that it has a hierarchy of plans linked to key performance indicators and has a well-developed quality management systems integrated with the Services' technical regulatory framework. The TFSPO adherence to the Service's regulatory framework resulted in the early development of approved plans and procedures for effective introduction into service and logistic support of ADF aircraft and aircraft-related equipment. In contrast, the Navy's FFGSPO's plans, key performance indicators and the regulatory compliance system were either under review or in the early stages of implementation, despite the Upgrade Program being nearly six years old. This, when combined with problems related to the project's software safety and testing program, is likely to result in delays in the technical certification of the Upgraded FFGs and as a result delays in their acceptance into service.

Theme 6 — Business Continuity Management

An important aspect of an entity's governance and risk management strategies is an assessment of the risk to the continued availability of service delivery and information. The assessment requires an entity to understand its operating environment, and the constraints and threats that could result in a disruption to services. This process is more commonly referred to as business continuity management.

The outcome of such an assessment requires entities to develop business continuity arrangements for those areas considered necessary for maintaining business operations. The objective of business continuity management is to ensure the availability of all key business resources required to support critical business processes in

the event when normal operating activities are affected by a disaster or disruption event.

In examining how well entities are addressing business continuity the ANAO concentrates on the following elements of business continuity management:

- business continuity policy, and its integration with entity governance and risk management policies;
- business continuity plans and processes as they contribute to the maintenance of business operations in the event of a disruption;
- incident reporting;
- continuity training and awareness; and
- disaster recovery plans (DRP) and processes that enable IT systems to be re-instated to a satisfactory operating level in a timely manner following a disruption event.

In most entities reviewed, management responsibility for business continuity had been identified and assigned, with roles and responsibilities clearly articulated. Business continuity plans, where completed, had been based on business impact analysis, with due consideration given to system criticality assessments.

However, a significant number of entities still have work to do to ensure they have developed, implemented, tested and documented comprehensive business continuity plans. While most entities had an appropriate business continuity policy in place, they had yet to complete supporting plans for all critical areas of their business. [71]

Concluding Remarks

I will conclude by observing that the revised standard issued by Standards Australia in August 2004 emphasises the point that risk management is an important element of an organisation's corporate governance.

A sound understanding of the major contributors to organisational risk assists in its management and in related communications. The framework set up by Atkinson[72] and referred to earlier in this paper is very useful, namely, considering the contributors to organisational risk in terms of strategic risk; environmental risk and operational risk. This framework then provides a focus for organisational efforts to manage risk.

The idea of integrating risk across an organisation and risk management being embedded in its culture is essential to the success of the risk management process. Among the most critical challenges is determining how much risk an entity is prepared to, and does, accept as it strives to implement the government's agenda and/or create value in the public sector. Organisations that effectively amalgamate elements of their risk and compliance activities can reduce costs and increase clarity of their operations.

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. Effective risk management requires a risk assessment culture that supports a holistic approach to the identification and management of risk throughout an organisation.

Additionally, risk management should be part of an organisation's strategy and planning processes, and an integral component of corporate governance. Importantly, an integrated risk management system develops the control environment, which provides reasonable assurance that the organisation will achieve its objectives with an acceptable degree of residual risk.

Internal audit can play a critical role in helping an organisation develop its strategic response to its changing risk profile and ensuring effective risk management processes are in place to respond quickly. Additionally, internal audit can play an important role in ensuring that the risk control framework is in place and operating as intended; internal audit also plays a complementary role in evaluating whether the controls are practical, whether they are functional and how they might be circumvented.

Risk management is central to the development and operation of an organisation's control structure and, therefore, of its corporate governance. 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[73].

In turn, 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.

Risk management needs to be actively applied. Critical risks and treatments should be closely reviewed by senior managers. 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.

Notes and references:

[1] 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

[2] Ibid

[3] Ibid, p27

[4] Ibid, pp27,28

[5] European Federation of Accounts, 2005, Discussion Paper, *Risk management and Internal Control in the EU*, p.8.

[6] Atkinson, Anthony A and Webb, Alan, *A Directors Guide to Risk and its Management*, Op.cit. p26

[7] Joint Committee of Public Accounts and Audit, 2000. *Contract Management in the Australian Public Service – Report 379*. The Parliament of the Commonwealth of Australia, Canberra. October. pp.80-87

[8] Victorian Auditor General, 2004, Better Practice Guide, *Managing risk across the public sector*, Melbourne, June, p.1

[9] ANAO Audit Report No 50 2004-05 *"Drought Assistance"*2 June 2005

[10] Shergold, Dr Peter, 2005, Launching *Foundations of Governance in the Australian Public Service*, 1 June, found at www.pmc.gov.au

[11] Ibid

[12] Australian Public Service Commission, 2005, *Foundations of Governance in the Australian Public Service*, p. 4.

[13] ANAO Audit Report No. 58, 2003-2004, *Control Structures as part of the Audit of Financial Statements of Major Australian Government Entities for the Year Ending 30 June 2004*, Canberra, 26 June 2004, p. 49

[14] McPhee, I 2002. *Risk Management and Governance*, Address to the National Institute for Governance, Canberra, 16 October.

[15] Deloitte Touche Tohmatsu, *Risk Management*, found at www.deloitte.com/dtt/section_node/0,sid%3D10268,00.html

[16] Lucas, Janet & Fulton, Tony, 2005, Tax Compliance: responding to a dynamic environment, Internal Tax Review, n7, July 2005, p. 56

[17] Gillian, Warren, 2005, Key Note Address, as reported in Australian Government Risk Manager, Issue No 21, Winter, p.1

[18] Banham, Russ, 2005, *Enterprising Views of Risk Management*, International Federation Of Accountants, Articles of Merit, August, p. 14

[19] Ibid

[20] Ibid

[21] Hughes, Peter, 2005, Risk Management and Assurance, Ernst & Young Risk Management Series, Fifth Edition, July , p.7

[22] Joint Committee of Public Accounts and Audit, 2000. *Contract Management in the Australian Public Service – Report 379*. OpCit. pp.80-87

[23] UK Committee of Public Accounts First Report, 2001-02 (HC 336), *Managing Risk in Government Departments*, as cited in the UK NAO's Report, *Managing Risks to Improve Public Services*, 22 October 2004, p3

[24] Jackson, Russell, 2005, *There is no good shortcut to good controls, Internal Auditor*, August, p. 63

[25] Risk Management, 2005, *Billions at risk through governance gaps*, Issue 19, July, p. 8

[26] Warga, Thomas, 2005, *Keeping our Promise*, Internal Auditor, August, p. 40

[27] Banham, Russ, 2005, *Enterprising Views of Risk Management*, International Federation of Accountants, Articles of Merit, August, p. 19

[28] ANAO Audit Report No. 58, 2003-2004, Op. cit, p. 11

[29] Ibid, p. 16

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

[31] Ibid

[32] found at www.number-10.gov.uk/SU/RISK/REPORT/01.HTM

[33] The UK Government Strategy Unit, 2002, *Risk: Improving government's capability to handle risk and uncertainty*, p. 1
[34] Ibid p.2
[35] ANAO Audit Report, No 54, 2003-04, Op cit, p. 60
[36] The UK Government Strategy Unit, 2002, Op cit, Chapter 2, p. 1
[37] Australian Risk Management Newsletter, 2004. *Lessons for all in NAB*, Vol 14 No 3. April. p.1.
[38] Ibid. p.4.
[39] Aon Limited, 2004, *Reputation Risk Management*, p. 1 found at www.aon.com/uk/en/about/topical_isssues/corporate_governance/reputation.jsp
[40] Moodie, Ann-Maree, 2005, *Charities: compliance risk gets bigger*, CFO Magazine, 1 May
[41] ANAO Audit Report, No. 17 2004-05, *The Administration of the National Action Plan for Salinity and Water Quality*, Canberra, 15 December 2004, p.38
[42] Drawn from the UK NAO, Report *Managing Risks to Improve Public Services*, 22 October 2004, pp 7-9.
[43] ANAO Audit Report, No. 14, 2004-05, *Management and Promotion of Citizenship Services, Canberra*, Canberra, 5 November 2004, p. 22
[44] ANAO Audit Report No. 56, 2004-05, *Interim Phase of the Audit of Financial Statements of General Government Sector Entities for the Year Ending 30 June 2005*, 24 June 2005, pp. 61-62
[45] ANAO Audit Report, No 40, 2004-05, *The Edge Project*, 14 April 2005
[46] ANAO Audit Report, No 8, 2005-06, *Management of the Personnel Management Key Solution (PMKeyS)* Implementation Project, 26 August 2005
[47] ANAO Report No 40, 2004-05, *The Edge Project*, Op cit
[48] ANAO Report No 8, 2005-06, *Management of the Personnel Management Key Solution (PMKeyS) Implementation Project*, Op cit.
[49] ANAO Audit Report, No 21, 2004-05, *Audits of the Financial Statements of Australian Government Entities for the Period Ended 30 June 2004*, Canberra, 12 January 2005, p. 29.
[50] ANAO Audit Report, No 45, 2004-05, *Management of Selected Defence System Program Offices*, 27 May 2005, p. 23
[51] ANAO Audit Report No 7, 2003-2004. *Record-keeping in Large Commonwealth Organisations*, Canberra, 24 September 2003, p.11.
[52] Ibid., p.15.
[53] Barry, Rick, 2004, *Web Sites as Recordkeeping & Recordmaking Systems*, The Information Management Journal, November/December 2004.
[54] Ibid, p. 27
[55] Ibid, p. 32
[56] Ibid, p. 32
[57] O'Keefe, Timothy P and Langemo, Mark 2005. *Controlling the Risks of Content Publication*, The Information Management Journal Vol 39, No 1 January/February, p.40
[58] Ibid., p.43
[59] ANAO Audit Report, No 18 2004-05, *Regulation of Non-prescription Medical Products*, Canberra, 16 December 2004.
[60] Ibid, pp 116 - 118
[61] ANAO Audit Report, No 54, 2003-04, *Management of the Detention Centre Contracts*—Part A, Canberra, 18 June 2004
[62] Ibid, pp 13-14
[63] Ibid, p.14
[64] Ibid, p 58
[65] ANAO Audit Report, No. 3, 2003-04, *The Management of Risk and Insurance*, Canberra, 27 August 2003
[66] Ibid, p.19
[67] Ibid, p.19
[68] Ibid, p.19
[69] Ibid, Appendix 2, pp 112-122
[70] ANAO Audit Report No 45, 2004-05, *Management of Selected Defence System Program Offices*, Op cit.

[71] ANAO Report No. 56, 2004-05, *Interim Phase of the Audit of Financial Statements of General Government Sector Entities for the Year Ending 30 June 2005*, Op. cit

[72] Atkinson, Anthony A and Webb, Alan, *A Directors Guide to Risk and its Management* Op.Cit pp 26, 27

[73] Barrett, P 2002. Expectation and Perception, of Better Practice Corporate Governance in the Public Sector from an Audit Perspective, Address to the CPA Australia's Government Business Symposium, Melbourne, 20 September.