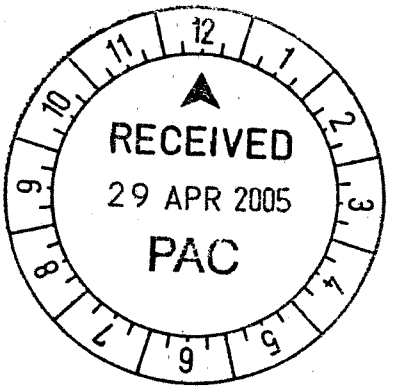
11

THE AUDIT OFFICE
OF NEW SOUTH WALES

CONTACT NAME R J Sendt
TELEPHONE 9275.7101
OUR REFERENCE A 1556
YOUR REFERENCE

Mr Matt Brown MP
Chairman
Public Accounts Committee
Legislative Assembly, Parliament House
Macquarie Street
SYDNEY NSW 2000



29 April 2005

Dear Mr Brown

PAC Inquiry into Risk Management

Please find attached a copy of the Audit Office submission into the Public Accounts Committee's inquiry into Risk Management in the NSW Public Sector.

Yours sincerely

R J Sendt
Auditor-General

AUDIT OFFICE OF NEW SOUTH WALES

SUBMISSION TO THE PUBLIC ACCOUNTS COMMITTEE
INQUIRY INTO RISK MANAGEMENT

Introduction

In the 1990s, the USA, Britain, Israel and other countries developed integrated risk management and internal control frameworks for organisations. The intent was that an organisation that effectively implemented these internal controls could be reasonably assured of managing its many operational, financial, legal and regulatory risks and meeting its objectives.

In NSW, Treasury took the lead in assisting agencies to assess and improve current internal control practices. In 1995 Treasury issued a guideline 'Best Practice on Internal Control and Internal Audit' and in 1997 it issued a 'Risk Management and Internal Control Toolkit'. These documents were developed from documents such as the 'Internal Control - Integrated Framework' (COSO I) developed in the USA by COSO: the Committee of Sponsoring Organizations of the Treadway Commission.

At the same time Standards Australia and Standards New Zealand developed and issued a new code - *AS/NZS 4360:1999 - Risk Management*. The Risk Management Standard was developed locally and has been widely adopted in Australia and New Zealand and also internationally.

Findings and Recommendations of the NSW Audit Office 2002 Audit of Risk Management

In June 2002 the Audit Office conducted an audit of risk management within the NSW public sector. The audit included a survey of 26 agencies. We concluded that:

> ... while agencies are aware of the need to manage risk, their risk management falls short of better practice. Many agencies do not consider their risk management to be adequate.
>
> The survey suggests that some agencies, mainly those in the Public Trading Enterprise Sector, have approached risk management in a systematic way and in accordance with the principles of better practice standards.
>
> Others, mainly government departments not subject to commercial imperatives, have yet to progress the management of risk beyond the traditional response of insuring against the more common types of risk'.

In our audit we also examined Annual Reports, because agencies are required to report on their management of risk in their Annual Reports. We found that in most cases it would not be possible for stakeholders, particularly Parliament, to make informed judgements from Annual Reports about the risks faced by agencies and the management of those risks.

We made a number of recommendations on improving risk management in agencies and on better public reporting by agencies. We also recommended that Treasury should have a continuing role oversighting risk management practice in agencies and encouraging the adoption of better practice.

Current Position

As we have not carried out a follow up audit of our 2002 audit of risk management, we do not have any new or specific recommendations to make for the Committee.

However we have retained an interest in the subject, and we have gleaned some observations in our ongoing contacts with NSW government agencies. Based on that knowledge we offer some comments below that may assist the Committee in its deliberations.

How the NSW public sector has responded to the recommendations of the Auditor-General's 2002 Report

Treasury's guidelines had been issued for several years when we carried out the 2002 audit. We found that interest in risk management was stronger in the Public Trading Enterprise (PTE) Sector than in the General Government Sector (GGS). For example, 73% of the PTEs we surveyed had a risk management policy against 46% of the GGS agencies. However we also found that 73% of the PTEs did not use the Treasury Toolkit.

Looking more closely at what was happening, we are inclined to think that our 2002 audit survey results may have picked up the early success of *AS/NZS 4360: Risk Management*, first issued in 1999. Since then, we have observed that both public and private organisations in Australia have continued to adopt *AS/NZS 4360:1999 Risk Management* and its recent update in 2004. It is quite possible that *AS/NZS 4360* has been the most influential variable in driving the increasing adoption of risk management in the NSW public sector.

How NSW public sector agencies are implementing the requirements of AS/NZS 4360

Although we have not researched this question, our impression is that NSW Government agencies, particularly the public trading sector enterprises, are increasingly implementing *AS/NZS 4360:Risk Management* to develop risk management as a core internal control process. They are applying it to program planning and to operations at many levels and some are also using it as the basis for developing enterprise risk management policies.

The launch of the updated Standard and expanded guidance material by Standards Australia in 2004 received considerable public sector attention, and appears to have further refreshed and consolidated the pre-eminence of the Standard locally.

The Standard has also made a significant impact overseas. It is relatively simple to understand and readily applied at many levels.

The level of progress towards developing a better risk management practice in the NSW public sector

In our 2002 audit we stated that:

> ... if the Toolkit is to be used more widely by the public sector, more effort is required by Treasury.

In response to our 2002 audit, Treasury said that it was:

> developing a Working Paper to initiate discussion with agencies about the characteristics of performance management systems necessary to support efficient and effective service delivery. This project will incorporate basis characteristics or standards of an effective risk management system.

Treasury has issued some further advice on risk management. For example, In October 2004 it issued a policy and guidelines paper for General Government agencies titled *What You do and Why - An Agency Guide to Defining Results and Services*. Section 3 contains guidance on risk management. However, as far as we are aware, Treasury has not updated the guidelines and toolkit on risk management and internal control that it issued from 1995 to 1997.

We believe that the AS/NZS Risk Management Standard has become very popular and is enjoying considerable use overseas as well as in Australian and New Zealand. The COSO model is less pervasive in Australia than in the USA, and we sense that in the NSW public sector the Treasury Toolkit (based on COSO I) has not established a strong presence.

(A 2004 KPMG survey of over 80 major private and public sector entities in Australian and New Zealand showed 50 per cent using the AS/NZS Standard and 36 per cent using COSO.)

With the 2004 release of COSO II, the Treasury Toolkit is arguably even less likely to be applied by agencies. The changes to the COSO model are considerable, moving from a pyramid framework to a more complex cube matrix model.

Suggestions on a Way Forward

We anticipate that risk management will increasingly be seen as a strategic issue. Agencies will need to align risk management with strategic objectives and corporate governance arrangements and to integrate it into business planning and reporting cycles.

Agencies will need guidance on how to implement this future direction. A need exists for a robust framework to effectively identify, assess and manage risk at a strategic level across an enterprise.

We see the central issue at present as - where will the agencies obtain the guidance they need to apply a risk management framework across their organisations?

This framework could be built on *AS/NZS:2004-Risk Management* and some of the supporting documents such as *Standards Australia's Guide to Controls Assurance and Risk Management (HB254-2003)*. Or it could be built on the recently published COSO II (Enterprise Risk Management - Integrated Framework). COSO II incorporates the internal control framework of COSO I but provides more guidance on enterprise risk management.

Although we have not made a detailed comparison of *AS/NZS 4360:2004* and COSO II, we have attended presentations that do so and the two models appear to be built on similar concepts. *AS/NZS 4360:2004* sets out a process for risk management that is applicable at many levels including enterprise level. COSO II describes in more detail how to implement enterprise wide risk management and how to integrate it with other internal control systems. Both seem to address some aspects of risk management not addressed, or not as well addressed, in the other. Possibly there will be a convergence between the two.

Those who use AS/NZS 4360 generally say it is a very workable, easily understood guideline. There should be no need to move away from it in the short term.

However COSO II also has its attractions. It has a USA source and is being adopted by global companies. It is also consistent with the approach of the Sarbanes-Oxley Act and similar legislation currently being enacted following the series of high profile business failures in the late 1990s and early 2000s. It has the potential to become the world standard.

Both approaches have merit. There are also other approaches being developed around the world, such as the Canadian (COCO) model and UK frameworks.

As the external auditor for the NSW public sector, we place great importance on agencies embracing risk management in a meaningful, practical way. We see some signs of this happening. But we think that it needs further stimulation, and a consistent approach in the sector would be desirable.

The Treasury Toolkit is now out of date and does not reflect current best practice, given that it is based upon COSO I which has since been significantly updated. If the Treasury guidelines and Toolkit are intended to be 'the standard' for NSW public sector agencies, they need to be updated now and on an on-going basis. An update could be based on either *AS/NZS 4360:2004* or COSO II (we would probably lean towards the former) or could include the best features of both. However this is a matter for Treasury to determine.

References

NSW Treasury

- Best Practice on Internal Control and Internal Audit - June 1995
- Risk Management and Internal Control Toolkit - September 1997
- Financial Management Framework for the General Government Sector
- OFM Policy and Guidelines Paper - 'What Do You do and Why? An Agency Guide to Defining Results and Services' - October 2004

Standards Australia (www.standards.com.au)

- AS/NZS 4360:2004: Risk Management (first issued 1999)
- HB436:2004 (Guidelines to AS/NZS 4360:2004): Risk Management Guidelines Companion to AS/NZS 4360:2004
- Standards Australia's Guide to Controls Assurance and Risk Management (HB254-2003)

COSO: Committee of Sponsoring Organizations of the Treadway Commission (www.coso.org)

- Internal Control - Integrated Framework (1992) (COSO I)
- Enterprise Risk Management - Integrated Framework - September 2004 (COSO II)

Risk Management Institution of Australasia

- 'Future Challenges for Risk Management in the Australian Public Sector' - Pat Barrett - Opening address at the RMIA ACT Chapter Conference 'Bringing Risk Management Together - What the Future Holds' Canberra 7 April 2005 (see www.anao.gov.au/WebSite.nsf/Publications/0CEA578630DF21EDCA256FDC007F9019)