Appendix three – About the audit

Audit objective

This audit examined how effectively government agencies are building risk management capabilities and embedding a sound risk culture throughout their organisation.

Audit criteria

We addressed the audit objective by examining the following:

1. Agencies can demonstrate that senior management has provided a mandate for, and is committed to, risk management (tone at the top).
2. Information about risk is communicated effectively throughout the agencies.
3. Agencies are building risk management capabilities.

Audit scope and focus

In assessing the criteria, we checked the following aspects:

1. Agencies can demonstrate that senior management has provided a mandate for, and is committed to, risk management (tone at the top).
   a) Senior management has endorsed a risk management framework and articulated the level of risks the agency is willing to accept.
   b) Risk management is integrated into the organisation's strategic planning process.
   c) Senior management engages with staff to foster a 'no blame' culture.
   d) Surveyed employees indicate they feel comfortable raising issues, challenging ideas and are encouraged by their senior managers to identify opportunities from future uncertain events.
   e) Risk related matters are included or operationally embedded in performance agreements.
   f) Key risk issues are discussed at senior leadership and Audit and Risk Committee meetings.
   g) Risk culture is monitored, measured, reported to senior management and continuously improved.
   h) Sufficient resources are allocated to the risk management function.

2. Information about risk is communicated effectively throughout the agencies.
   a) The organisation has comprehensive, relevant and timely risk reporting.
   b) There is communication of 'good' and 'bad' news.
   c) The risk register identifies the organisation's key risks and is regularly updated to reflect the most current risk information, including lessons learnt from past events.
   d) Executive decision-making demonstrates that relevant/material risks and rewards are considered.
   e) Business units, the risk management function, compliance, internal audit and other control functions have clearly delineated responsibilities regarding monitoring, identification, management and escalation of risk. These functions are coordinated so that there are neither 'gaps' in controls nor unnecessary duplications of coverage.
   f) Surveyed employees at all levels indicate they are aware of risks in their business, how to respond to them, the boundaries of risk taking and the objectives of their role.

37

NSW Auditor-General's Report to Parliament | Managing risks in the NSW public sector: risk culture and capability | Appendix three – About the audit

3. Agencies are building risk management capabilities.

    a) Responsibility for building risk management capability throughout the organisation is well defined and proportionally resourced.

    b) Risk management training is well targeted, and provided both at induction and on an ongoing basis throughout employment.

    c) Surveyed employees at all levels view risk management as adding value, outcomes based, easy to understand.

This audit focused on key risks that have the potential to impact - either in a positive or negative way - on the success of the entire organisation.

The audit looked at the NSW Police Force, the NSW Fair Trading function within the Department of Finance, Services and Innovation, the Ministry of Health, and NSW Treasury Corporation (TCorp). NSW Treasury was also an auditee because of its role in supporting agencies to develop and implement risk management frameworks and processes. NSW Treasury's internal risk management processes and frameworks were not being audited.

Audit exclusions

The audit did not:

- assess agencies' compliance with core requirements of TPP 15-03
- conduct a detailed audit of the quality of risk assessments of projects and programs
- question the merits of Government policy objectives.

Audit approach

Our procedures included:

1. Interviewing Agency Heads of NSW Police Force, DFSI, TCorp, the Ministry of Health and NSW Treasury.

2. Interviewing relevant staff within NSW Police Force, DFSI, TCorp and the Ministry of Health responsible for:
   - developing and implementing risk management frameworks and plans
   - strategic planning
   - internal audit function
   - risk management function
   - risk management training
   - human resources and recruitment
   - project management office.

3. Interviewing executives from a sample of business units within NSW Police Force, DFSI, TCorp and the Ministry of Health.

4. Interviewing relevant staff within NSW Treasury responsible for developing policy and guidelines to support agencies to develop and implement risk management frameworks (e.g. TPP 12-03 and TPP 15-03).

5. Consultation with other stakeholders, including:
   - APRA
   - icare
   - Suncorp Risk Services
   - Public Service Commission.

6. Surveying employee's views on risk management and risk culture.

7.   Analysing data, including:
   - agency data collection (staff surveys, complaints data, records of attendance at risk management training modules, key risk indicators, and risk management course evaluations).

8.   Examining key documentation, including:
   - risk management frameworks, policies, plans, procedures and reports
   - risk registers
   - risk appetite statement
   - a sample of incident reports
   - agenda papers and minutes from Audit and Risk Committees
   - a selection of internal communication
   - a selection of strategic planning documentation and decision-making structures
   - annual reports
   - risk management training programs
   - agenda papers and minutes from selected senior management meetings
   - risk management training modules and workshop materials
   - organisational charts
   - a selection of job descriptions and performance agreements.
   - documentation from other stakeholders obtained throughout the audit such as research and studies, statistical data and analysis
   - information from other jurisdictions for comparison and better practice guidelines.

The audit approach was complemented by quality assurance processes within the Audit Office to ensure compliance with professional standards.

Audit methodology

Our performance audit methodology is designed to satisfy Australian Audit Standards ASAE 3500 on performance auditing. The Standard requires the audit team to comply with relevant ethical requirements and plan and perform the audit to obtain reasonable assurance and draw a conclusion on the audit objective. Our processes have also been designed to comply with the auditing requirements specified in the *Public Finance and Audit Act 1983*.

Acknowledgements

We gratefully acknowledge the co-operation and assistance provided by the Ministry of Health, the Department of Finance, Services and Innovation, NSW Police Force, NSW Treasury Corporation and NSW Treasury.

Audit cost

The cost of the audit was approximately $340,000 including overheads and travel costs.

39

NSW Auditor-General's Report to Parliament | Managing risks in the NSW public sector: risk culture and capability | Appendix three – About the audit