auditoffice
OF NEW SOUTH WALES

# Managing risks in the NSW public sector: risk culture and capability

23 APRIL 2018

NEW SOUTH WALES AUDITOR-GENERAL'S REPORT

PERFORMANCE AUDIT

# THE ROLE OF THE AUDITOR-GENERAL

The roles and responsibilities of the Auditor-General, and hence the Audit Office, are set out in the *Public Finance and Audit Act 1983* and the *Local Government Act 1993*.

We conduct financial or 'attest' audits of State public sector and local government entities' financial statements. We also audit the Total State Sector Accounts, a consolidation of all agencies' accounts.

Financial audits are designed to add credibility to financial statements, enhancing their value to end-users. Also, the existence of such audits provides a constant stimulus to entities to ensure sound financial management.

Following a financial audit the Audit Office issues a variety of reports to entities and reports periodically to parliament. In combination these reports give opinions on the truth and fairness of financial statements, and comment on entity compliance with certain laws, regulations and government directives. They may comment on financial prudence, probity and waste, and recommend operational improvements.

We also conduct performance audits. These examine whether an entity is carrying out its activities effectively and doing so economically and efficiently and in compliance with relevant laws. Audits may cover all or parts of an entity's operations, or consider particular issues across a number of entities.

As well as financial and performance audits, the Auditor-General carries out special reviews and compliance engagements.

Performance audits are reported separately, with all other audits included in one of the regular volumes of the Auditor-General's Reports to Parliament – Financial Audits.



GPO Box 12
Sydney NSW 2001

The Legislative Assembly
Parliament House
Sydney NSW 2000

The Legislative Council
Parliament House
Sydney NSW 2000

In accordance with section 38E of the *Public Finance and Audit Act 1983*, I present a report titled '**Managing risks in the NSW public sector: risk culture and capability'.**

**Margaret Crawford**
Auditor-General
23 April 2018

auditoffice
OF NEW SOUTH WALES

audit.nsw.gov.au

# contents

## Managing risks in the NSW public sector: risk culture and capability

# Section one

## Managing risks in the NSW public sector: risk culture and capability

# Executive summary

Effective risk management is essential to good governance, and supports staff at all levels to make informed judgements and decisions. At a time when government is encouraging innovation and exploring new service delivery models, effective risk management is about seizing opportunities as well as managing threats.

Over the past decade, governments and regulators around the world have increasingly turned their attention to risk culture. It is now widely accepted that organisational culture is a key element of risk management because it influences how people recognise and engage with risk. Neglecting this 'soft' side of risk management can prevent institutions from managing risks that threaten their success and lead to missed opportunities for change, improvement or innovation.

This audit assessed how effectively NSW Government agencies are building risk management capabilities and embedding a sound risk culture throughout their organisations. To do this we examined whether:

- agencies can demonstrate that senior management is committed to risk management
- information about risk is communicated effectively throughout agencies
- agencies are building risk management capabilities.

The audit examined four agencies: the Ministry of Health, the NSW Fair Trading function within the Department of Finance, Services and Innovation, NSW Police Force and NSW Treasury Corporation (TCorp). NSW Treasury was also included as the agency responsible for the NSW Government's risk management framework.

## Conclusion

All four agencies examined in the audit are taking steps to strengthen their risk culture. In these agencies, senior management communicates the importance of managing risk to their staff. They have risk management policies and funded central functions to oversee risk management. We also found many examples of risk management being integrated into daily activities.

That said, three of the four case study agencies could do more to understand their existing risk culture. As good practice, agencies should monitor their employees' attitude to risk. Without a clear understanding of how employees identify and engage with risk, it is difficult to tell whether the 'tone' set by the executive and management is aligned with employee behaviours.

Our survey of risk culture found that three agencies could strengthen a culture of open communication, so that all employees feel comfortable speaking openly about risks. To support innovation, senior management could also do better at communicating to their staff the levels of risk they are willing to accept.

Some agencies are performing better than others in building their risk capabilities. Three case study agencies have reviewed the risk-related skills and knowledge of their workforce, but only one agency has addressed the gaps the review identified. In three agencies, staff also need more practical guidance on how to manage risks that are relevant to their day-to-day responsibilities.

NSW Treasury provides agencies with direction and guidance on risk management through policy and guidelines. Its principles-based approach to risk management is consistent with better practice. Nevertheless, there is scope for NSW Treasury to develop additional practical guidance and tools to support a better risk culture in the NSW public sector. NSW Treasury should encourage agency heads to form a view on the current risk culture in their agencies, identify desirable changes to that risk culture, and take steps to address those changes.

# 1. Key findings

### Senior management communicates the importance of managing risks

We surveyed staff and found that 65.5 per cent of surveyed employees reported that senior leaders communicated that managing risks effectively is a priority in their agency.

Senior management sets the expectations for the risk culture of an organisation. To gain insights into how this is happening in practice, we interviewed 48 executives and managers from the four case study agencies and found that senior management in all four agencies acknowledge the importance of managing risks as a central part of their role.

### More could be done to strengthen a culture of open communication

Across the four case study agencies, an average of 17.8 per cent of surveyed employees reported that if things went wrong they would not feel safe in calling these out. Another 12.5 per cent of staff neither agreed nor disagreed that they would feel safe doing so. When even a small number of people are deterred from calling out issues, opportunities to share learnings and improve outcomes are missed.

The survey results varied significantly across the agencies we reviewed. In one case study agency, 93.2 per cent of staff reported they would feel safe in reporting incidents to management, with another 3.4 per cent of staff indicating that they neither agreed nor disagreed that they would feel safe doing so. In this agency, risk management was consistently championed by the managers and executives we interviewed. This example demonstrates that other agencies could also do more to foster a culture of open communication.

### There is scope to expand the role of the chief risk officer to provide 'effective challenge'

In three agencies we reviewed, we found that the chief risk officer or equivalent does not have a formal role in challenging risk decisions within the agency. This contrasts with a trend that is emerging in the private sector following the 2008 global financial crisis, in which challenging senior management and business lines is expected.

While providing 'effective challenge' should be encouraged at all levels of an organisation, the chief risk officer is particularly well placed to perform this function. There is scope to extend this role in the public sector to challenge ideas and provide different perspectives in decision-making.

### Some agencies are starting to adopt a more proactive approach to managing risks

Most agencies we examined are seeking to develop a more forward-looking approach to managing and anticipating risks.

We found examples of agencies using data analytics as a tool to examine trends and identify risks. This is an area that is expected to grow as agencies invest more heavily in digital technology and data management.

Proactive approaches seek to identify all relevant risks earlier, before an incident occurs, and take the required steps to avoid them. This can be done by monitoring risks on an ongoing basis through a review of incidents and by focusing on finding root causes and early warning indicators.

### Agencies are taking steps to develop a holistic view of risks

Not all agencies we examined were using the central risk function to coordinate and report to senior executives on high-level risks. We found examples of risks being managed in silos with little involvement of the central risk function.

Senior management in these agencies acknowledged this issue and are taking steps to develop a more holistic view of the risks they face by strengthening their enterprise risk management programs. If implemented well, these initiatives will help senior management understand the key challenges they face.

Integrating disparate risk reporting within agencies could provide senior management with a more consistent view of the key risks across the agency. It also allows for a better understanding of the interdependencies between risks.

### Information on enterprise-wide risks could be better linked to decision-making

Three agencies we reviewed could not consistently demonstrate that risk information collected by the central risk function was used to improve decision-making.

For example, corporate risk registers developed by agencies to document information about risks to their corporate objectives, were not consistently used as a tool to support decision-making. Not having a clear purpose for reporting risks can undermine the development of a sound risk culture.

In these agencies, enterprise risk management focuses on compliance with NSW Treasury policy 'TPP 15-03 Internal Audit and Risk Management Policy for the NSW Public Sector'. In addition to achieving compliance, good risk management depends on creating a culture where staff meaningfully engage with risk and this is considered a fundamental part of decision making.

### Most agencies do not monitor or measure risk culture

Only one of the four agencies we reviewed explicitly monitored, measured, and reported on risk culture to senior management.

As good practice, agencies should monitor and measure their employees' attitude to risk. Without clear measures of their risk culture, it is difficult to know whether the 'tone' set by the executive and management is reflected in employee's behaviours throughout the organisation. Measuring risk culture also helps agencies identify the gaps between the current and desired culture, and target interventions at those areas that will produce the greatest benefits.

### A principles-based approach to managing risks is consistent with better practice

NSW Treasury provides agencies with direction and guidance on risk management through policy and guidelines. Its principles-based approach to risk management is consistent with better practice. Under this approach, agencies must tailor their risk management frameworks to meet their specific needs.

Nevertheless, there is scope for NSW Treasury to develop additional practical guidance and tools to help agencies strengthen their risk culture. As good practice, NSW Treasury should encourage agency heads to form a view on the current risk culture in their agencies, identify desirable changes to that risk culture, and take steps to address those changes.

## 2. Recommendation

**By May 2019, NSW Treasury should:**

Review the scope of its risk management guidance, and identify additional guidance, training or activities to improve risk culture across the NSW public sector. This should focus on encouraging agency heads to form a view on the current risk culture in their agencies, identify desirable changes to that risk culture, and take steps to address those changes.

## 3. Sector-wide learnings

Through research, interviews and analysis conducted as part of this audit, we have identified learnings that agencies across the sector could consider to embed a risk culture throughout their organisation.

### Leadership

- Before changing risk culture, senior management needs to develop a view of their agencies' existing organisational culture, as well as their target risk culture for the organisation.
- Heads of agencies will be best placed to make decisions and provide advice when they have relevant and reliable information on risks at their disposal.
- Risk management as a discipline is an enabler and cannot replace leadership. Risk management tools give a framework but are not a substitute for good judgement.
- While formal training plays a role in building risk management capability, there remains a place for insights based on experience and shared learnings.
- Risk management, when used well, is a tool that can help senior management focus on the issues that really matter.

### Communication

- The Chief Risk Officer plays a crucial role in driving a sound risk culture by translating the concepts of risk management into language easily understood by line-managers. Further, it is critical for them to build strong relationships with other functions across the agency.
- It is important that agencies communicate lessons learnt to staff who can benefit from them, rather than moving on quickly from problems or mistakes without reflecting on how things could have been done better.
- In rapidly changing times, it is important to update risk registers regularly to capture new and emerging risks and close off on past issues.
- Informal, open and frequent communication from staff to line managers plays a key role in developing a sound risk culture.

### Identification of risks

- Proactively identifying risks allows agencies to prepare and deal with issues before they turn into larger problems.
- It is important to win support for risk management from the line managers who conduct the agency's day-to-day business. They may be in a better position to identify emerging threats.
- There is a distinction between risk aversion and risk ignorance. If risks are not proactively identified, agencies may take large risks without being aware that this is the case.
- Extensive knowledge of an organisation's operating environment plays a significant role in identifying the most relevant risks'.
- While enterprise risk management is mainly the preserve of senior executives, all staff should be capable of identifying and managing risks.
- Building risk resilience is fundamental for an agency to respond to the unpredictable and adapt to a rapidly changing environment.

# 1. Introduction

## 1.1 Background

### Managing risk within the context of government

Government agencies are responsible for a range of activities, from policy making, regulating businesses and delivering services to the community. All these activities involve a degree of risk.

To be effective in managing risks, an agency needs to consider its internal and external operating environment. Different parts of government need to manage risks in ways that are tailored to their circumstances, and commensurate with the scale and nature of their risk profile.

Traditionally agencies have focused on managing operational risks. As well as operational risks, agencies also face strategic risks. These risks cut across the enterprise and often include factors that cannot be totally controlled within the agency.

Managing risks in the public sector is a complex task for many reasons, including:

- it involves dealing with many stakeholders, who often have different tolerances for risk
- governments are increasingly required to tackle complex policy problems
- an interconnected world and a 24-hour news cycle create pressure for quick action
- government is using new service delivery models in partnership with the private and not-for-profit sectors. This creates risks associated with the commissioning process
- risk aversion can prevent agencies from innovating and seizing opportunities.

### What is the government's risk management framework?

In 2009, NSW Treasury released the 'TPP 09-05 Internal Audit and Risk Management Policy for the NSW Public Sector'. This policy sought to strengthen internal audit, risk management and governance processes. An updated policy was released in 2015.

NSW Treasury's policy outlines broad principles for effective risk management (Exhibit 1). This is in line with the international standard on risk management (AS/NSZ ISO 31000:2009, Risk Management Principles and guidelines). A principles-based approach aims to empower agencies by providing flexibility to achieve policy objectives. It also places responsibility on agencies to manage their own risks and decide on the approaches that best meet their needs.

**Exhibit 1: Principles of effective risk management**


Source: TPP15-03, adapted from AS/NSZ ISO 31000:2009, Risk Management Principles and guidelines.

## Risk culture and capability

Many NSW public sector agencies have designed policies and procedures for dealing with risks. However, a risk management policy is not in itself sufficient evidence that an agency has implemented effective risk management practices.

A core component of a risk management framework is risk culture. The Australian Prudential Regulation Authority defined risk culture as:

> 'the influence of organisational culture on how risks are managed in an organisation. It is how staff identify, understand, discuss and act on the risks an organisation confronts and takes.'

High-level assessments conducted by the Audit Office of New South Wales in 2017 indicated that many agencies could strengthen their risk culture (Exhibit 2).

**Exhibit 2: The Audit Office's 2017 assessment of risk management maturity**

Our 'Report on Internal Controls and Governance 2017' assessed the risk management maturity level of 39 agencies using the Audit Office's 'Risk Management Maturity Assessment Tool'. Five assessment criteria were used to assess agencies' risk management maturity:

- Strategy and governance
- Process
- Systems and intelligence
- Monitoring and review
- Culture.

We found that all agencies have risk management frameworks with varying levels of maturity. When reviewed against five critical assessment criteria, agencies fared best in strategy and governance, but most need to improve their risk culture, systems and intelligence. For more details see: https://www.audit.nsw.gov.au/publications/latest-reports/internal-controls-and-governance-2017.

A key aspect of embedding a risk management culture into an organisation is staff capability. This refers to the knowledge, skills and abilities that public sector employees must demonstrate to perform their roles effectively. Building risk capability is a key management function. In doing this, agencies get support and guidance from NSW Treasury and icare.

NSW Treasury produced a range of guidance material to help agencies develop and implement risk management processes. NSW Treasury's Risk Management Toolkit includes templates, checklists and practical advice on various elements of the policy.

icare supports agencies by:

- providing learning and development programs to build organisational risk capability
- coordinating awards and organising seminars
- facilitating networking opportunities between agency risk practitioners
- assisting agencies assess the maturity of their systems for managing risk.

In addition, the NSW Public Sector Capability Framework provides a common foundation for creating and recruiting to roles, managing performance, capability development, career planning and workforce planning in the NSW public sector. The Capability Framework identifies 'being proactive to address risks' as a behaviour that is expected of all public-sector employees.

The NSW Public Sector Commission has also developed occupation-specific capability sets to support the Capability Framework. The Finance Professionals Capability Set includes risk management as one of seven capabilities, while the Procurement Capability Set includes the ability to manage procurement risks.

## About this audit

This audit assessed how effectively NSW Government agencies are building risk management capabilities and embedding a sound risk culture throughout their organisation. We examined whether:

- Agencies can demonstrate that senior management is committed to risk management
- Information about risk is communicated effectively throughout the agencies
- Agencies are building risk management capabilities.

To do this, the audit reviewed four agencies:

- Ministry of Health
- NSW Fair Trading
- NSW Police Force (Corporate Services Division)
- NSW Treasury Corporation (TCorp).

The audit also examined the role of NSW Treasury as it is the central agency responsible for promulgating policy and guidelines in this area.

As part of the audit, we:

- interviewed senior management in five agencies
- reviewed documentation relating to the risk management frameworks and related material in the four agencies
- conducted a survey of staff in the four agencies, with a total of 418 responses.

See appendix three for more on the audit scope, criteria and methodology.

# 2. Key findings

In assessing an agency's risk culture, we focused on four key areas:

**Executive sponsorship (tone at the top)**

In the four agencies we reviewed, senior management is communicating the importance of managing risk. They have endorsed risk management frameworks and funded central functions tasked with overseeing risk management within their agencies.

That said, we found that three case study agencies do not measure their existing risk culture. Without clear measures of how employees identify and engage with risk, it is difficult for agencies to tell whether employee's behaviours are aligned with the 'tone' set by the executive and management.

For example, in some agencies we examined we found a disconnect between risk tolerances espoused by senior management and how these concepts were understood by staff.

**Employee perceptions of risk management**

Our survey of staff indicated that while senior leaders have communicated the importance of managing risk, more could be done to strengthen a culture of open communication so that all employees feel comfortable speaking openly about risks. We found that senior management could better communicate to their staff the levels of risk they should be willing to accept.

**Integration of risk management into daily activities and links to decision-making**

We found examples of risk management being integrated into daily activities. On the other hand, we also identified areas where risk management deviated from good practice. For example, we found that corporate risk registers are not consistently used as a tool to support decision-making.

**Support and guidance to help staff manage risks**

Most case study agencies are monitoring risk-related skills and knowledge of their workforce, but only one agency has addressed the gaps it identified. While agencies are providing risk management training, surveyed staff in three case study agencies reported that risk management training is not adequate.

NSW Treasury provides agencies with direction and guidance on risk management through policy and guidelines. In line with better practice, NSW Treasury's principles-based policy acknowledges that individual agencies are in a better position to understand their own risks and design risk management frameworks that address those risks. Nevertheless, there is scope for NSW Treasury to refine its guidance material to support a better risk culture in the NSW public sector.

**Recommendation**

By May 2019, NSW Treasury should:

- Review the scope of its risk management guidance, and identify additional guidance, training or activities to improve risk culture across the NSW public sector. This should focus on encouraging agency heads to form a view on the current risk culture in their agencies, identify desirable changes to that risk culture, and take steps to address those changes.

## 2.1 Executive sponsorship (tone at the top)

### Agency heads acknowledge the importance of managing risks

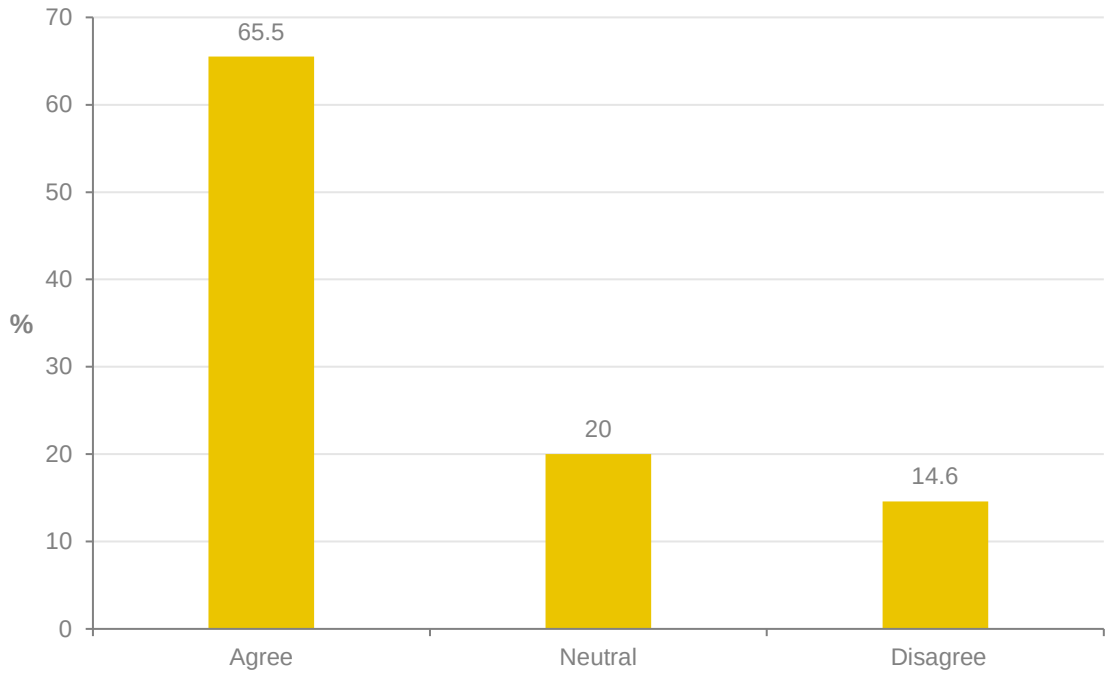
Agency heads play a fundamental role in driving risk management in the NSW public sector. They are the starting point for establishing the expectations for the risk culture of an organisation. In addition, responsibility and accountability for risk management and the operation of an agency rests primarily with them.

We interviewed the heads of four agencies, who told us they show their commitment to risk management in many ways, including:

- prioritising risks
- frequently communicating the importance of managing risks to members of the executive and their teams
- appointing members of the executive who bring different perspectives and are capable of challenging existing views in a constructive way
- supporting initiatives designed to improve organisational culture and seeking to shift the focus to continuous learning rather than attribution of blame
- acknowledging that 'the buck stops with them' and taking responsibility for mistakes of more junior staff
- rewarding risk-taking and innovation even where it is not fully successful (e.g. Exhibit 3)
- seeking regular input from the Chief Risk Officer on the agency's top risks
- revisiting the risk management framework and assessing whether it remains fit-for-purpose during organisational change
- properly resourcing the risk management function.

Senior management's stated commitment to managing risks is supported by staff feedback. We surveyed staff and found that nearly two out of three employees reported that senior leaders communicated that managing risks effectively is a priority in their agency (Exhibit 3).

**Exhibit 3: Senior leaders in my agency have communicated that effectively managing risks is a priority**



Most managers and employees also agree that risk management adds value to their organisations (Exhibit 4).

**Exhibit 4: Risk management adds value to my organisation**

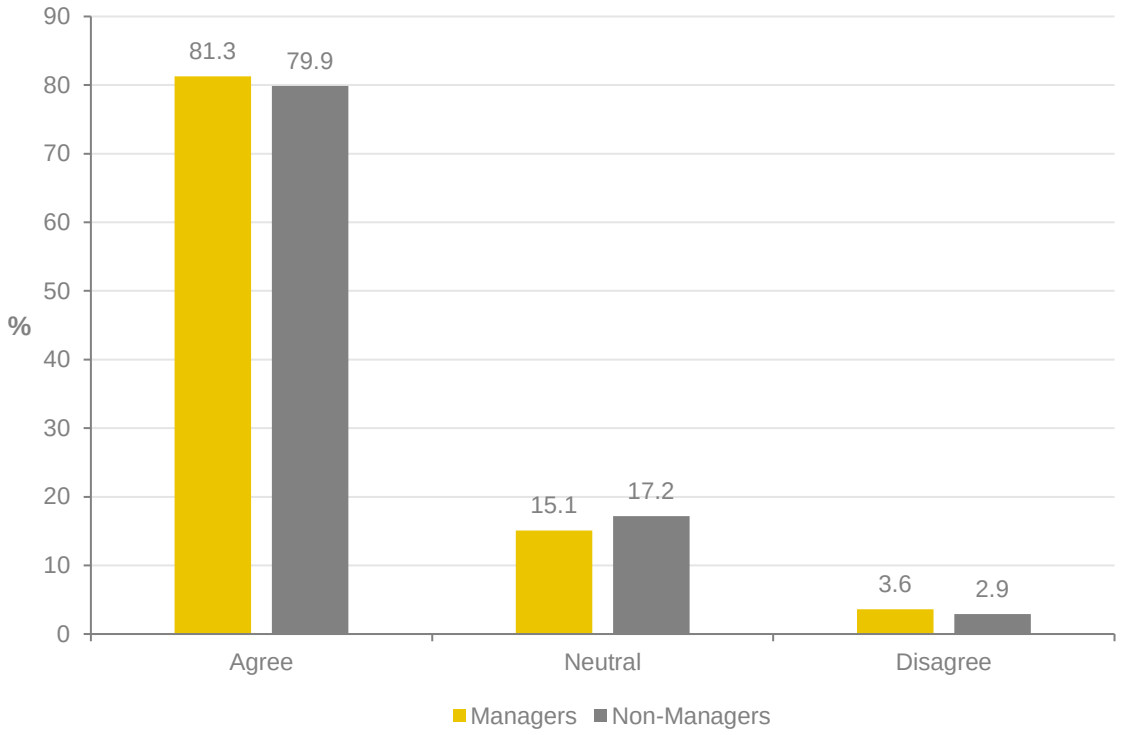



**Exhibit 5: Supporting innovation and risk taking: 'Dare to Try' award**

In 2016, the Department of Finance, Services and Innovation launched the 'Dare to Try - Creating an Innovation Mindset' award. The purpose of the award is to recognise those who take some risks in launching a new initiative or project, even if it is not as successful as intended. By doing this, the department seeks to encourage employees and teams to try innovative approaches, even if this involves a degree of measured risk-taking.

In the first year, the Dare to Try award was won by the SafeWork NSW farm safety campaign 'Alive and Well'. Alive and Well was developed to inform farmers and their families about the risks and dangers of living and working on the farm.

## Agencies have designed frameworks for managing risks

Risk management frameworks outline the overall approach for managing risks throughout an organisation. Establishing a framework for managing risks that supports the agency's objectives is a core requirement of NSW Treasury's policy TPP15-03. In line with better practice, NSW Treasury encourages agencies to tailor those frameworks to meet their specific needs.

Three of the four agencies we examined have up-to-date frameworks for managing risks. Common elements of risk management frameworks include:

- a risk appetite statement
- a description of roles and responsibilities for managing risks
- a description of the process for managing, monitoring, reporting and reviewing risks
- risk categories
- risk rating matrices.

Most agencies we reviewed are also continuing to develop elements of their risk management framework to respond to changes in their internal and external environments.

## Staff reported the risk management function is adequately resourced

A well-resourced risk function is a key indicator of senior management commitment to risk management. We reviewed the annual budget and staffing for the central risk management function and interviewed key senior staff. In three of the four case study agencies, staff reported the risk management function is adequately resourced for its current function.

The number of resources varied depending on the size, complexity and type of agency. For example, one agency had recently hired extra risk staff. Another agency was in the process of upgrading its risk reporting system, which it expected would relieve some of the burden on existing staff.

Currently, it is common for the Chief Risk Officer to have multiple roles; for example, they may oversee governance, risk and compliance. This arrangement can help with streamlining processes and optimising resources. However, if not carefully implemented, it can lead to risk management being considered a low priority, and allow less time for activities that may impact on the agency's risk profile.

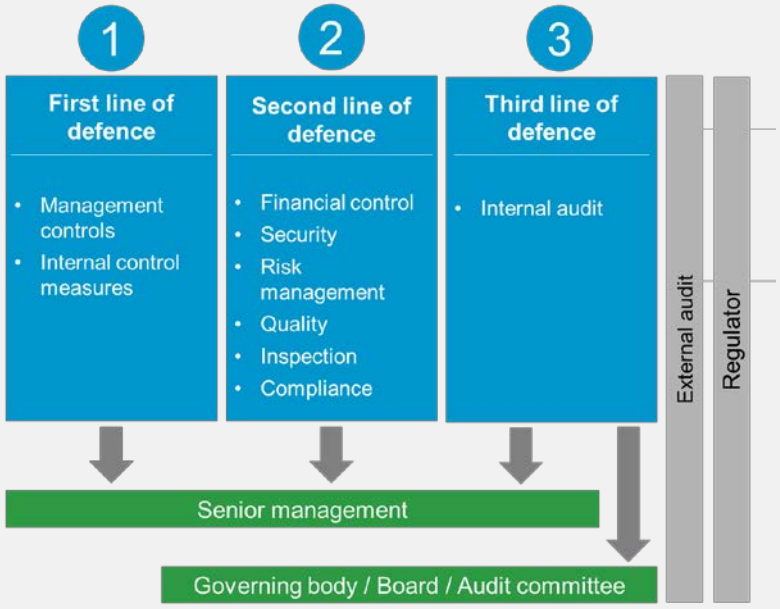
## Chief Risk Officers have sufficient access to senior executives

The Chief Risk Officer is typically the person appointed to lead the risk function within the agency. We found that the Chief Risk Officer or equivalent was either a member or reported to a member of the executive team in three of the agencies we examined. In the remaining agency, the person in this role developed an effective communication channel with the head of the agency. It is considered good practice that responsibility for risk management be assigned to an officer at a senior level, with sufficient authority and access to the executive leadership team.

To better define responsibilities and coordinate control functions, most agencies are moving towards a 'three lines of defence' model (Exhibit 6).

**Exhibit 6: The 'three lines of defence' model**

Under a three line of defence model, primary responsibility for risk management – the first line of defence – rest with the business units undertaking day-to-day operations. That is, the first line 'owns' and manages the risks. The second line of defence reviews and challenges the first line. This is generally delivered through oversight committees, specialist enterprise risk and compliance functions, which are independent from the first line of defence. The third line of defence gives independent assurance that the first and second lines are working effectively. This is typically supplied by an internal audit function.




Adapted from Audit Committees: A guide to good practice, Third Edition. Australian Institute of Company Directors.

### The central risk function is underutilised

Not all agencies we examined were effectively using the central risk function to coordinate and report to senior executives on the agencies' strategic risks.

In most agencies we reviewed, only a few strategic risks were regularly included on the agenda of senior executive meetings. Further, when strategic risks were discussed at the executive level, they were not always aligned to key risks identified in the corporate risk register.

Most senior management would benefit from receiving more regular and comprehensive information on the agencies' key risks from the central risk function. Integrating disparate risk reporting within agencies and making better use of the central risk function would give senior management a more holistic view of the key risks across the agency and controls in place. It would also allow for a better understanding of the interdependencies between the risks.

### Risk culture is rarely monitored or measured

Only one out of four agencies we reviewed explicitly monitored, measured, and reported on risk culture to senior management. This agency used internal audit to assess and gain insights into their risk culture. It conducted workshops, surveyed employees and benchmarked results against similar organisations.

Without monitoring the risk culture, it is difficult for senior management to understand whether their views on how risks should be managed are supported by the agency's culture more broadly. Without a sufficient understanding of the risk culture of an agency, it is also difficult to target interventions to those areas that produce the greatest impact.

Each year, the Public Service Commission surveys all employees across the NSW Government through the People Matter Employee Survey. The survey includes some indicators of a culture of open communication. For example, the 2017 edition asked employees if they were in a position to speak up and share a different view to their colleagues and managers. Its broader focus on workplace performance means that the People Matter Employee Survey only gives a partial view of the risk culture in an agency.

The focus on monitoring risk culture has been emphasised in the financial industry sector. In 2015, the Australian Prudential Regulation Authority (APRA) introduced the Prudential Standard CPS 220 Risk Management (CPS 220) requiring each board of an APRA regulated organisation to form a view of the risk culture in the institution, identify any desirable changes to that risk culture, and ensure the institution takes steps to address those changes.

## 2.2 Employee perceptions of risk management

### A proportion of employees are still reluctant to speak openly about risks

Of the four agencies we reviewed, we found that on average 17.8 per cent of employees who responded to our survey reported that if things went wrong they would not feel safe in calling these out. Another 12.5 per cent of staff neither agreed nor disagreed that they would feel safe doing so. When even a small number of people are deterred from calling out issues, opportunities to share learnings and improve outcomes are missed.

In one case study agency, 93.2 per cent of staff reported they would feel safe in reporting incidents to management, with another 3.4 per cent indicating that they neither agreed nor disagreed that they would feel safe to do so. In this agency, risk management was consistently championed by the managers and executives we interviewed.

These results were consistent with responses to other questions in our survey (see Appendix two for full survey results). In addition, the Public Service Commission's 2017 People Matter Survey asked employees if they can speak up and share a different view to their colleagues and manager. The survey found that across the NSW public sector 66 per cent of employees felt comfortable doing so, compared to 69 per cent in the previous year.

This indicates that the NSW public sector still has a way to go in creating a culture that encourages and legitimises open discussions. Without a culture of open communication, an organisation cannot focus on learning from what went wrong and make sure mistakes are not repeated. Further, establishing a speak up culture creates checks and balances and leads to better decision-making.

That said, agencies we audited had several initiatives aimed at improving organisational culture. Many aimed to encourage a respectful culture. Having a respectful culture can give more confidence for staff to speak openly, which would include speaking openly about risks. These initiatives include:

- Respectful Workplace Behaviours Initiative at NSW Police
- Statement of agreed principles on a respectful culture in medicine in health
- Incorporating behavioural expectations around raising issues into their performance agreements at DFSI (Exhibit 11).

**Exhibit 7: Public Service Commission's guidance on promoting open speak-up cultures**

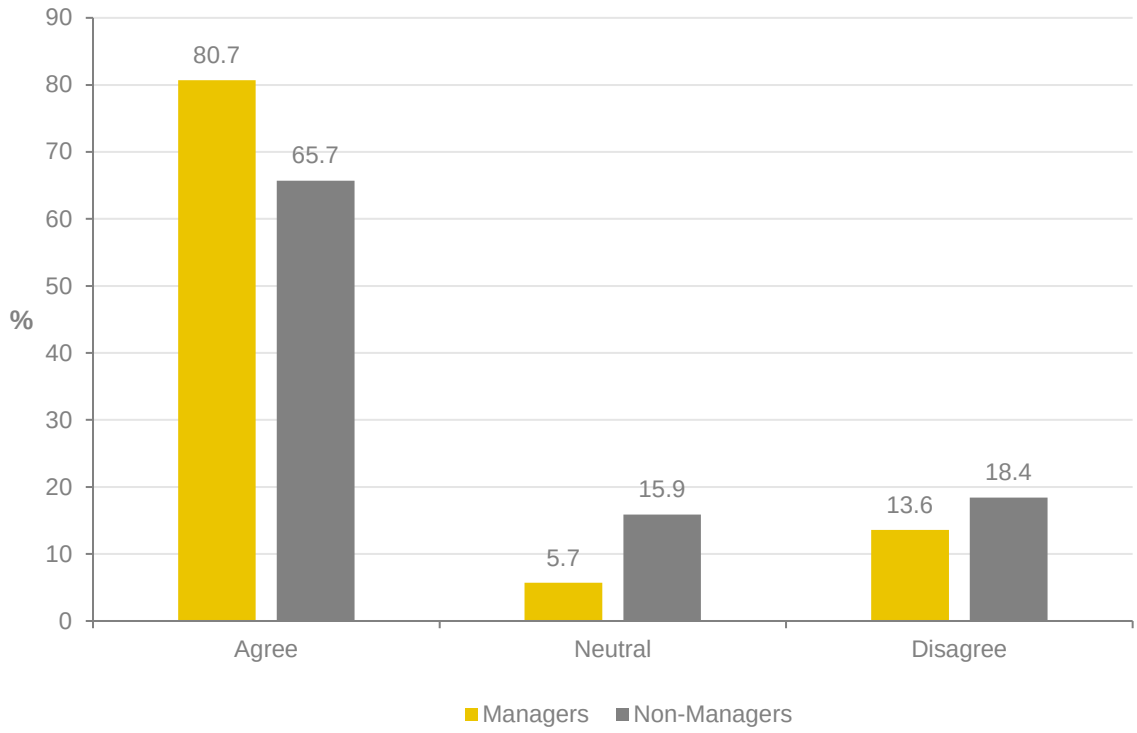
The Public Service Commission suggests a range of actions, systems and practices that can help agencies develop their open speak-up culture:

- Leadership and culture - Senior management should 'walk the talk' by:
    - being receptive to others' opinion, points of view and suggestions
    - expecting their agencies to have an open speak-up culture and practices
    - encouraging frank and fearless advice from staff
    - ensuring that staff recognise that, once a decision is made, employees are expected to implement that decision.
- Governance arrangements - The agency has ethics policies and procedures, as well as individuals responsible for implementing and monitoring them.
- Human resources - Recruitment, professional development and promotion practices encourage open speak-up practices.
- Communications - Internal and external communication should include good open speak-up practices including dialogue, feedback, and frank and fearless advice.
- Measurement - The agency measures indicators of an open, speak up culture and practices.
- Continuous improvement - The culture, leaders and practices encourage learning from best practice and look to implement that.

## There is a significant gap between how safe managers and non-managers feel when calling out issues in their work group

We found that managers generally feel safer in calling out issues than non-managers. (Exhibit 8). Further work is needed to close this gap because risks reported by non-managers are as valid as those raised by managers, and all staff are expected to be actively involved in risk management.

**Exhibit 8: If things go wrong in my work group, I feel safe in calling these out**



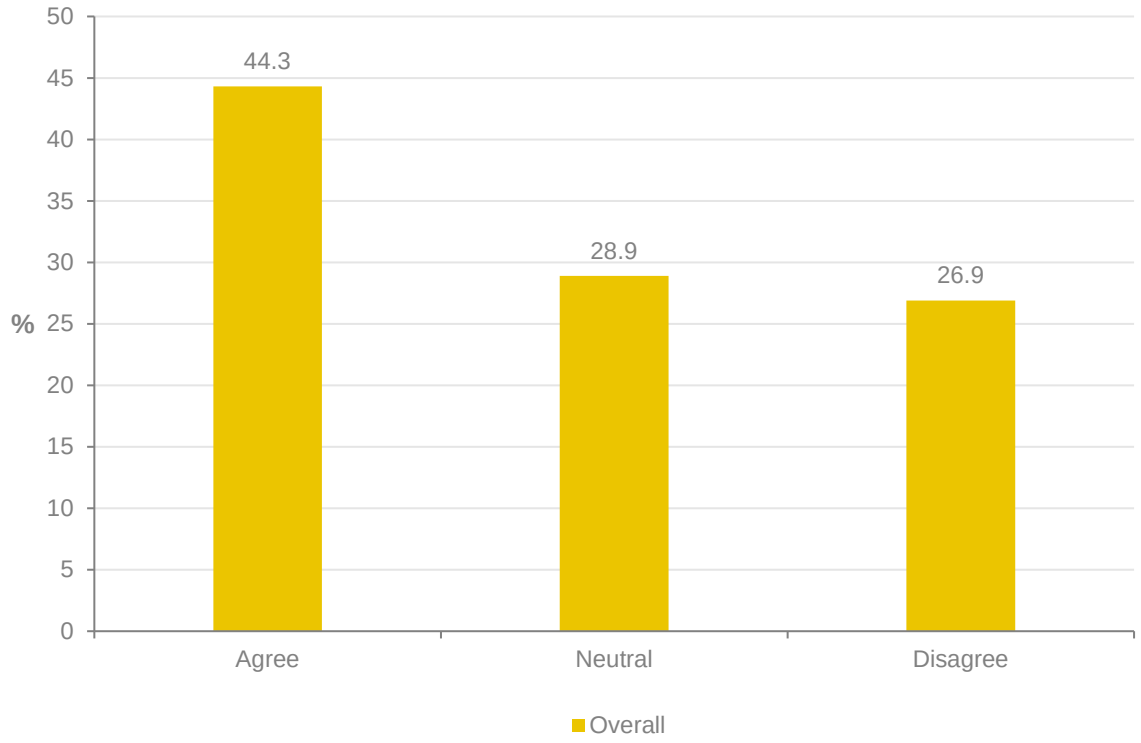

## Senior management is not effectively communicating how much risk it is acceptable to take

Risk tolerances refer to the maximum amount of risk an organisation is willing to accept for each type of risk it faces. This can be particularly useful if agencies want to foster innovation, as trying new ways of doing things requires a certain degree of risk-taking.

In some agencies we examined, we found a disconnect between risk tolerances espoused by senior management and how these concepts were understood by staff. We encountered examples where senior management reported seeing value in some risk-taking activities, such as trialling new infrastructure delivery models, while key staff supported a blanket approach of avoiding all risks at all cost.

Further, less than half of surveyed employees indicated that senior management had communicated the amount of risk that it was acceptable to take in their job (Exhibit 9). Specifying the maximum risk that an agency is willing to take regarding each relevant risk is important because it defines how people should respond to risks and the level of control that is required. Developing a shared understanding of the level of risk that an agency is prepared to accept also helps staff approach decision-making in a consistent way.

**Exhibit 9: Senior leaders in my agency make clear how much risk people in my work group are permitted to take when making decisions**

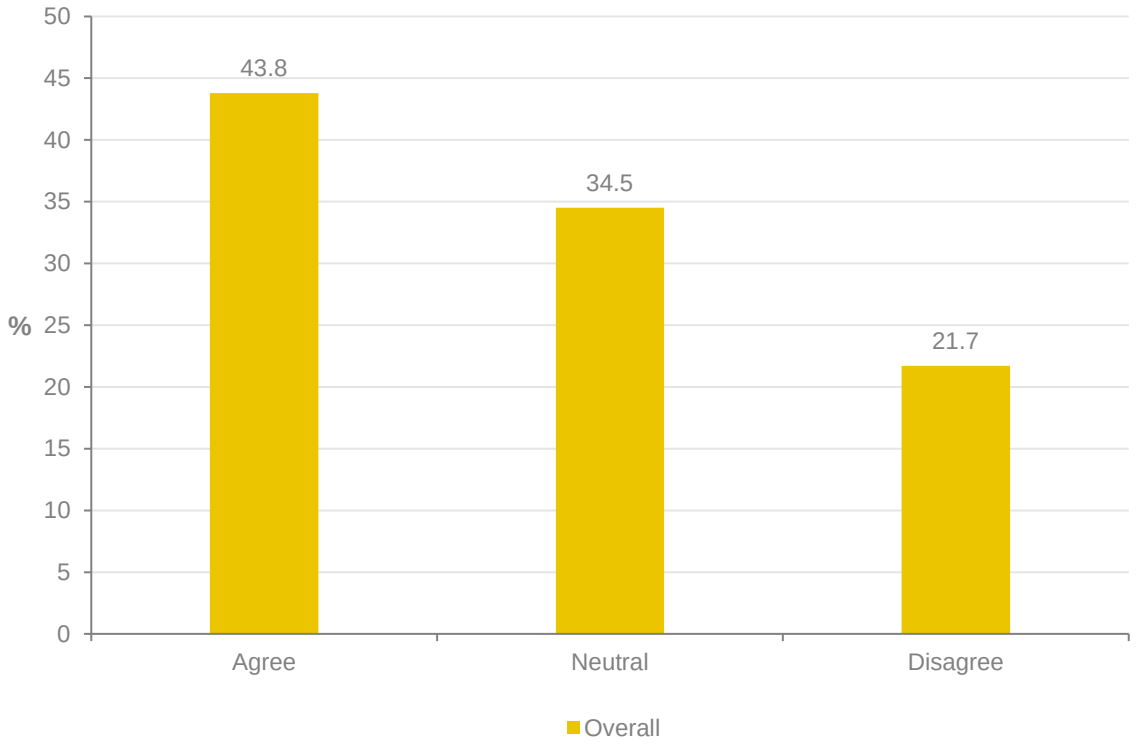



## Positive recognition for proactively managing risks could be strengthened

Financial and non-financial incentives play a significant role in supporting a sound risk culture by encouraging desirable risk management behaviours.

However, some agencies lack a strong incentive system that rewards employees based on the anticipation and management of risks. Only 44 per cent of surveyed employees agreed that they would be rewarded if they managed risks effectively in their day to day job (Exhibit 10).

**Exhibit 10: If I manage risks effectively in my day to day job I get positive recognition in my performance reviews**




One way of strengthening the incentives for managing risks is by incorporating risk into performance agreements of senior staff. For example, the Department of Finance, Services and Innovation includes risk management in the performance agreements of its executives (Exhibit 11).

**Exhibit 11: Incorporating risk into performance objectives**

The Department of Finance, Services and Innovation has introduced risk-related performance objectives for all its executives. The initiative aims to ensure that all executives see risk management as their responsibility and that they foster a culture where their staff are willing to raise risk. These performance objectives include:

- ensure risks are appropriately identified, captured, assessed and reviewed at least quarterly consistent with the Risk and Resilience Framework, including that a current risk register is in place for your business
- ensure staff are aware of their risk accountabilities and risks are regularly communicated internally and externally to your business and reported where necessary
- ensure risk is integrated in key decision-making processes including business unit planning, project management, employee wellbeing and safety, and finance/budget management
- foster a culture where staff raise risk (positive and negative) by implementing reward and recognition strategies to encourage good risk management practices (e.g. celebrating success through communication strategies, rewards through projects, secondments, high potential rotations, education and training).

## 2.3 Integrating risk management into daily activities and decision-making

### Risk management is embedded in several core business activities

Agencies are embedding risk management into a variety of day-to-day activities. These activities include:

- conducting risk assessments to better identify the level of threat to a victim of domestic and family violence
- on-going monitoring of clinical risk through review of clinical incidents and 'root cause analysis'
- monitoring of credit, liquidity and market risks
- focusing compliance activities on the groups that carry the highest risk of non-compliance
- introducing health promotion and injury prevention programs for workers dealing with dangerous situations and attending traumatic scenes.

Agencies are planning to expand the use of risk-based approaches in corporate areas. This includes auditing, workforce strategic planning, procurement, and compliance. For example, New South Wales Police Force is starting to use data to better manage risks when allocating staff. (Exhibit 12).

**Exhibit 12: A risk-based approach to workforce planning: The Workforce Optimisation Solution for Policing**

NSWPF is introducing the Workforce Optimisation Solution for Policing (WOSP), a new workforce allocation model to inform workforce planning decisions. By directing resources to those areas of greatest need, the new system is designed to improve police performance overall and reduce the risks for the community.

The model focuses on measuring workload against current staffing levels. In the context of workforce planning, demand is composed of workload, coverage and risk. Many staffing issues arise from the perception that there is an overwhelming level of workload which does not match current staffing levels, and that the best solution is to add more staff. However, having the right people, at the right place and at the right time are all equally significant in addressing demand.

In consultation with the workforce, NSWPF established a standard measure of workload across similar organisational units and calculated resource requirements based on workload data. This system enables NSWPF to compare workloads across similar units, recommends staffing level based on workload and indicates where resources are needed most. This helps NSWPF be better informed in how it can re-allocate its resources.

### Implementation of enterprise risk management is progressing

Enterprise risk management refers to the application of risk management to all levels of an organisation and the development an agency-wide view of the risks it faces.

Three of the agencies we examined are in the early stages of implementing a risk management program across the enterprise. Currently, these agencies handle most risks at a business unit level, with limited reporting to the executive of high-level risks that affect the entire enterprise.

Senior management in these agencies acknowledged this issue and reported taking steps to improve the way they manage enterprise risks. If implemented well, these initiatives will create a more coordinated approach to managing risks and help agencies understand their key challenges.

**Exhibit 13: The Ministry of Health: implementation of an enterprise risk management program**

The Ministry of Health is in the initial stages of implementing a renewed approach to enterprise risk management, focusing on developing a system view of key risks and enhanced alignment between system risks and NSW Health's Strategic Objectives. This initiative also seeks to better integrate the risk function with the system performance and internal audit frameworks, and aims to use the Enterprise Risk Management framework to draw insight from risks managed locally by NSW Health Organisations across the system to inform The Ministry's Strategic Risk Profile.

The structure and focus of enterprise risk management varies according to an agency's size, responsibilities and complexity of its operations. Managing risk in a holistic manner, rather than treating each business unit individually, helps agencies identify shared risks and develop a consistent understanding of the most important risk areas.

### Risk registers are not consistently used as a tool to support decision-making

We found that high-level corporate risk registers, developed by agencies to document information about risks to their corporate objectives, are not consistently used as a tool to support decision-making and often become an end in themselves.

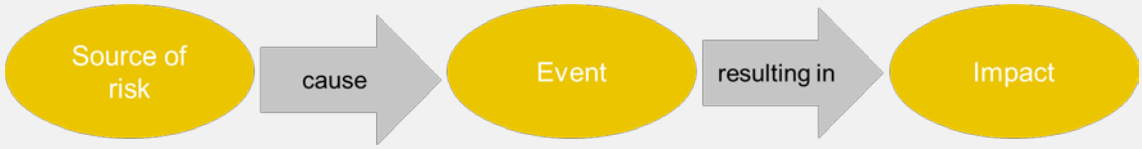
Complying with relevant policies is an essential element of good governance. However, treating the risk register as a 'tick-a-box' exercise to complete, without a clear link to better outcomes, may not lead to a proper discussion about the agency's risks and create a false perception of control.

We also found examples where corporate risk registers deviated from good practice. Some risk registers did not include full descriptions of risks and controls, and all relevant risks. Further, some risks were not regularly updated to reflect changing circumstances.

Risk registers play a key role in communicating information about risk to senior management. To help with decision-making, risk information should be communicated in a timely, accurate and understandable manner (Exhibit 14). To allow senior managers to focus on the key areas, it also needs to be prioritised and concise.

### Exhibit 14: Writing clear risk descriptions

Clear risk descriptions are important for ensuring that those who are not involved in identifying the risk can easily understand what the risk is, as well as ensuring that the risks themselves are clearly defined. While risks can be described in numerous ways, one method is as follows:




Adapted from TPP12-03: Risk Management Toolkit for NSW Public Sector Agencies.

Examples of clear risk descriptions:

- insufficient consultation with agency leads to Cabinet making a decision that impacts on the agency's operations, resulting in a resource shortfall
- ineffective change management results in reduced workplace efficiency, impacting on agency's ability to achieve strategic objectives
- lack of preparation and training leads to poor response to a potential high-profile public incident, impacting stakeholder support
- lack of effective service partnership management with other agencies leads to compromise of data, resulting in service breakdown
- ineffective ethical practice management results in fraud, which damages reputation and stakeholder support.

By ensuring that the risk description includes the source, event and impact, it is possible to know at a glance all the key information about the risk. If more detailed information is sought, then the reader can consult the rest of that entry on the risk register.

## Some agencies are adopting a more proactive approach to managing risks

Most agencies we examined are seeking to develop a more forward-looking approach to managing and anticipating risks.

Some agencies are investing in systems to collect data and track trends that will help them identify potential issues in advance, and take the required steps to avoid them.

### Exhibit 15: Using data analytics to understand trends: NSW Fair Trading

Illegal tenancy is a severe problem affecting large cities in NSW, which can lead to overcrowding, property damage, fire safety and health issues.

To target regulation more efficiently, NSW Fair Trading has partnered with the Data Analytics Centre to better understand the trends, early indicators and characteristics of illegal tenants. By using data analytics, it will be easier to identify illegal tenants, resulting in a more effective use of resources when prosecuting them.

Another illustration of a proactive approach to managing risks comes from within NSW Health. The Ministry of Health has sought to improve the quality and safe delivery of healthcare by introducing initiatives that identify and prevent circumstances that put patients at risk of harm (Exhibit 16). By doing this, it is moving away from a reactive approach to risk management, which focuses on responding to events after they have occurred.

**Exhibit 16: Open disclosure within NSW Health facilities**

The Ministry of Health has an open disclosure policy setting out the minimum requirements for a consistent open disclosure process within NSW Health. The initiative seeks to create a supportive environment where patient safety incidents are identified and reported without the attribution of blame. It also promotes sharing lessons learned from patient safety incidents to identify and develop strategies to prevent potential incidents.

Open disclosure is a critical element of early response and investigation of serious patient safety incidents. The policy encourages clinicians to apologise to a patient following a patient safety incident, without attribution of blame, and to record the incident in both the patient's health care record and the incident management system.

When a patient has been harmed because of a safety incident, an investigation will follow. The investigation team is responsible for determining the underlying causes that may have contributed to the patient safety incident. Where causes are identified that have contributed to the incident, the investigation team recommends quality improvement actions to address these issues, which aim to prevent recurrence. The specialist unit will then oversee their implementation and monitor the effectiveness of interventions.

## There is scope to expand the role of the chief risk officer to provide 'effective challenge'

In three agencies we reviewed, we found that the chief risk officer or equivalent does not have a formal role in challenging risk decisions within the agency.

In the private sector, the role of the Chief Risk Officer is constantly evolving. As well as implementing an enterprise risk management framework, the emerging trend is to give the Chief Risk Officer authority to review functions throughout the business and challenge any decision that is made.

There are merits in extending the role of the Chief Risk Officer in the public sector to provide effective challenge of senior management. Open communication and constructive challenge are key elements of a sound risk culture. While these behaviours should be encouraged at all levels of an organisation, the Chief Risk Officer is particularly well placed for providing effective challenge of ideas. There are several reasons for this, including:

- visibility of key risks impacting the agency
- established relationships with senior management and business units
- a good understanding of the agency's risk appetite
- independence from day-to-day management
- play a leadership role in promoting risk management across the agency.

## 2.4 Support and guidance to help staff manage risks

### Agencies provide risk management training at induction and on an ongoing basis

All agencies we reviewed offer some form of risk management training at induction. Those agencies which do not have generic risk management training available at induction offer related training, such as workplace health and safety. Most agencies also offer risk management training on an ongoing basis.

Risk management will be more effective when all staff are aware of their responsibilities and how to execute their roles. Although everybody is responsible for managing risks, the competencies that are required change as individuals progress through their career and their level of experience grows.

### Most agencies make risk management training compulsory

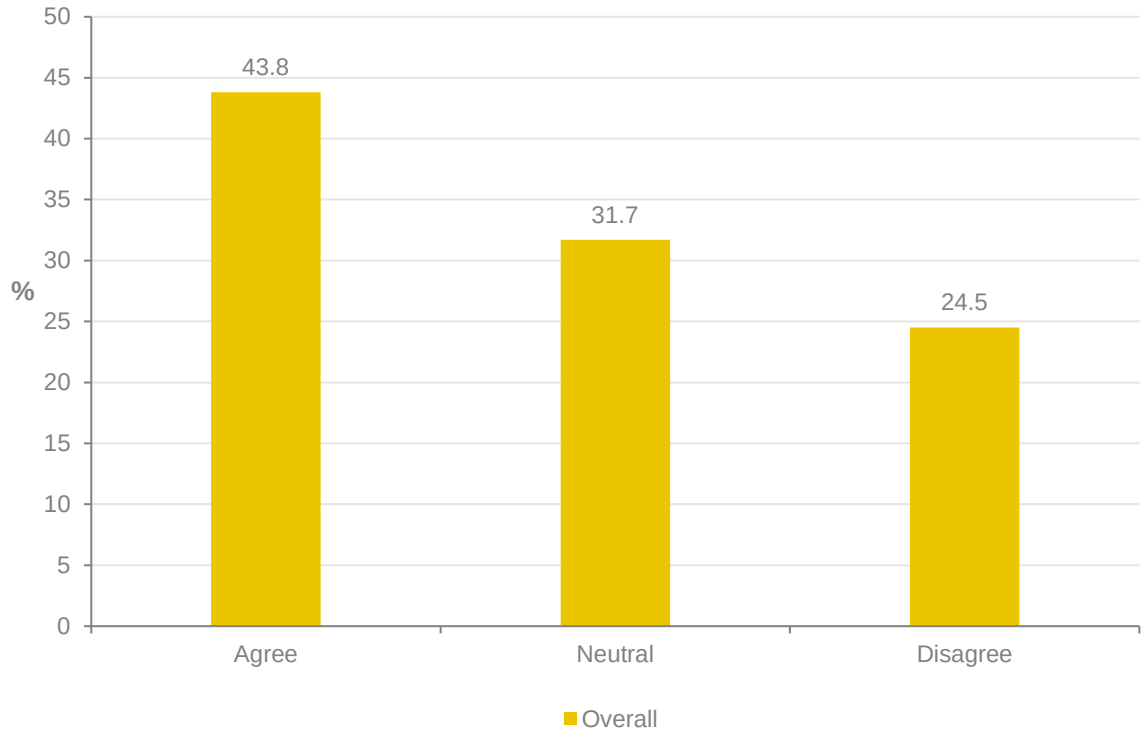
It is considered good practice that risk management training be a mandatory part component of continuing professional development. While we found that this is generally the case, in some agencies compulsory risk management training is limited to a few roles or targets specific areas such as health and safety.

At the same time, training courses are most effective when they are tailored to the needs of both the agency and the individual. For example, some agencies offer specific risk awareness training covering their legislative obligations, consequences of non-compliance, the type of risks they face and related process and procedures. We also found that agencies are using a variety of methods to deliver risk management training. This includes employing online modules, face-to-face training and delivering formal presentations at town hall meetings.

### A significant proportion of staff report that risk management training is not adequate

Despite training being mandatory and provided at induction and on an ongoing basis, only 43.8 per cent of surveyed staff agreed that they have got adequate training in risk management to perform their day-to-day tasks well (Exhibit 17). Another 31.7 per cent of surveyed employees neither agreed nor disagreed that they had received adequate training.

**Exhibit 17: I receive adequate training on how to manage risks to people, assets and service delivery to perform my day to day job well**



Results varied across the agencies we reviewed. In one agency, nearly 75 per cent of surveyed staff agreed that they received adequate training on how to manage risks to perform their day to day job well. The other three agencies would benefit from providing more practical guidance and training to staff on how to manage risks that are relevant to their day-to-day responsibilities.

Several factors may contribute to the perception of the level of training being inadequate in an organisation, including:

- some courses are not available to a broader range of participants. For example, one agency offered risk management training only to members of the risk function, even though other executives had related risk management responsibilities such as updating risk registers
- unavailability of training programs tailored to the needs of the agency or the individual. While there are several external providers of short training courses in risk management, this training tends to be very general rather than fit for purpose solutions
- unclear responsibilities for building risk management capability. We found that only two agencies we reviewed had clearly defined responsibilities for building risk capabilities.

### Some agencies are monitoring the risk-related skills and knowledge of their workforce

Three of the agencies have recently reviewed risk-related skills and knowledge of their workforce and identified gaps in their risk management capabilities. One agency has addressed the gap while the other two reported that they are in the process of implementing a solution. Evaluating risk capabilities on a regular basis will help agencies decide if their needs are being met.

One agency identified gaps in its risk capability, and filled these gaps by hiring staff with the required expertise. Another agency is proposing to fill its risk capability gap through training. The third agency is proposing to introduce a new system that will automate existing manual processes. The agency expects this to improve risk reporting and analytics capability.

### A principles-based approach to managing risks is consistent with better practice

NSW Treasury provides agencies with direction and guidance on risk management through policy and guidelines. Its principles-based approach to risk management is consistent with better practice.

A principles-based approach seeks to empower agencies by giving them greater flexibility in deciding how they will achieve stated policy objectives. Part of the rationale behind this approach is to shift the regulatory focus from process to outcomes. NSW Treasury's principled-based framework to managing risks is also consistent with a devolved model of accountability.

To support agencies to develop and implement their risk management framework, NSW Treasury has developed a Risk Management Toolkit (NSW Treasury Policy & Guidelines Paper TPP 12-03). The toolkit provides detailed and practical advice on various elements of ISO 31000, templates and some worked examples based on a hypothetical agency.

That said, there is scope for NSW Treasury to develop additional practical guidance and tools to help agencies strengthen their risk culture. NSW Treasury could play a greater leadership role by encouraging agencies to form a view on their current risk culture and identify any changes to it that could improve behaviour.

### NSW Treasury's role in supervising risk management in the NSW public sector is consistent with a principles-based approach

Enterprise risk management in most NSW public sector entities is governed by NSW Treasury's Internal Audit and Risk Management Policy for the NSW Public Sector (TPP 15-03). TPP15-03 requires agencies to comply with the core requirements of the policy, and to give an attestation to this effect to NSW Treasury on an annual basis.

NSW Treasury’s current approach to oversight of enterprise risk management in the public sector is limited to monitoring compliance with TPP15-03’s attestation statements and providing individual support in response to agency requests. This is consistent with a principles-based approach.

## The interface between NSW Treasury and agencies on risk management could be improved

The interface between NSW Treasury and public-sector agencies on risk management is complex. Public sector entities need to meet the risk management requirements set out in various pieces of legislation and NSW Treasury policies. Further, there are several entities and areas within NSW Treasury cluster that have a role in risk management (Exhibit 18). Agencies reported this could lead to duplication and make it difficult for public sector entities to understand their obligations.

**Exhibit 18: Treasury cluster and related entities with responsibilities for risk management**

| Entity and division | Responsibilities |
|---|---|
| NSW Treasury – Financial Risk Management and Transformation (FRMT) | Establish a new financial risk management capability in NSW Treasury.<br>Move the State towards risk, investment and performance-based resource allocation.<br>Some policies relate to risk management. For example, TPP 07-7 Commercial Policy Framework: Treasury Management Policy concerns the management of risks associated with NSW Treasury's functions. |
| NSW Treasury – Financial Management and Accounting Policy Branch | TPP 15-03 Internal Audit and Risk Management Policy for the NSW Public Sector is the overarching policy for risk management in the NSW public sector.<br>TPP 12-03 Risk Management Toolkit for NSW Public Sector Agencies (the Toolkit) provides guidelines, templates and a case study to assist individual agencies implement the requirements of TPP 15-03 and ISO 31000.<br>TPP 17-06 Certifying the Effectiveness of Internal Controls over Financial Information offers guidance, checklists and template for the assessment of controls over financial reporting risks.<br>TPP 16-02 Guidance on Shared Arrangements and Subcommittees for Audit and Risk Committees allows eligible agencies increased flexibility in the way in which they meet the requirements of TPP 15-03.<br>TPP 17-08 Requirements for Issuing, Managing and Reporting Instruments of Assurance includes specific risk management requirements over the issuance and management of guarantees and letters of comfort.<br>Prequalification Scheme for Audit and Risk Committee Independent Chairs and Members assists agencies with engaging ARC members with appropriate skills and experience, including those related to risk management. |
| icare Self Insurance | Provide specialised risk management services to agencies in their insurance schemes with the objective of improving risk management capability and the long-term resilience of the NSW public sector. Most of these services are outsourced to Suncorp Risk Services. All services provided by Suncorp Risk Services will be provided by icare Self Insurance effective 30 June 2018. |

| Entity and division | Responsibilities |
| --- | --- |
| Suncorp Group Limited – Suncorp Risk Services | Contracted by icare Self Insurance, the administrator of the NSW Government's managed fund schemes, to assist with building risk management capability in the sector. This is done through the following:<br>• developing and delivering learning and development programs<br>• organising seminars<br>• facilitating networking opportunities between agency risk practitioners<br>• assisting agencies assess the maturity of their systems for managing risk<br>• coordinating the annual awards and biannual conference programs<br>• providing support and advice. |

# Section two

Appendices

# Appendix one – Response from agencies

## Response from Ministry of Health

NSW GOVERNMENT Health

Ms Margaret Crawford
Auditor-General
Audit Office of NSW
GPO Box 12
SYDNEY NSW 2001

**Our ref** S18/142

Dear Ms ~~Crawford~~ Margaret.

**Performance Audit report on Managing Risks in the NSW Public Sector: Risk Culture and Capability**

Thank you for your letter of 13 March inviting NSW Health to provide a formal response on the Auditor-General's performance audit report on Managing Risks in the NSW Public Sector: Risk Culture and Capability.

The Ministry welcomes the report and the focus given to improve risk management culture and capability in the NSW Public Sector. As outlined in your report, the Ministry is currently working through a revision of our approach to risk management with a particular focus on how to best utilise risk information in decision making and to guide planning for our Health Services. Central to this work will be the fostering of a stronger risk management culture within NSW Health. Participation in this performance audit has provided insights which will inform our ongoing approach.

I appreciate the Ministry being a focus of two exhibits within the final report and for the opportunity to provide additional examples. I would also like to thank the auditors for working closely with the Ministry staff on this audit.

Yours sincerely

Elizabeth Koff
**Secretary, NSW Health**
3/4/18

NSW Ministry of Health
ABN 92 697 899 630
73 Miller St North Sydney NSW 2060
Locked Mail Bag 961 North Sydney NSW 2059
Tel. (02) 9391 9000 Fax. (02) 9391 9101
Website. www.health.nsw.gov.au

# Response from Department of Finance, Services & Innovation

Finance, Services & Innovation
NSW GOVERNMENT

McKell Building – 2-24 Rawson Place, Sydney NSW 2000
Tel 02 9372 8877 | TTY 1300 301 181
ABN 81 913 830 179 | www.finance.nsw.gov.au

**Office of the Secretary**

Our ref: BN 18/723
Your ref: 0006-00163

Ms Margaret Crawford
Auditor-General of NSW
Audit Office of NSW

via email: margaret.crawford@audit.nsw.gov.au

Dear Ms Crawford *Margaret*

**Final report on the performance audit: Managing risks in the NSW Public Sector: risk culture and capability**

Thank you for providing an opportunity to provide comments on the final performance audit report, "Managing risks in the NSW public sector: risk culture and capability", dated March 2018, prepared by the NSW Auditor General's Office.

Four agencies including the NSW Fair Trading function were examined as part of the audit. The report identifies 8 key findings which are non-agency specific and one recommendation for NSW Treasury to consider.

As you would be aware, I place a great emphasis on risk management within the Department and whilst the key findings were based on the audit of NSW Fair Trading, DFSI considers the findings have merit for implementation across the cluster and we have subsequently developed overarching strategies and a plan of action to address the key findings. These strategies include:

1. Improving the communication and understanding of risk management at all levels across DFSI through the development and implementation of a risk communication strategy and plan.
2. Improving the risk culture across the DFSI cluster to foster a culture where risks and issues are discussed and managed openly, using maturity evaluations and the communications strategy to engage with staff on risk.
3. Developing a culture which supports the Chief Risk Officer to challenge risks, through review of divisional risks as part of the quarterly review process or other mechanisms.
4. Improving the proactive management of risk through the identification and use of data analytics and other early warning indicators.
5. Improving the reporting of risks across the DFSI cluster to encourage improved management of interdependent and shared risks by investigating options to systemise reporting.
6. Develop training and tools to enable managers to make better risk decisions.
7. Capturing quantifiable metrics to understand risk culture and develop actions to improve reporting and behaviours.

8. Continuing to refine and develop the DFSI risk management policy and framework to ensure that risk culture is monitored and managed so that decisions are based on an understanding of the associated risks.

In addition to addressing the findings of the final Performance Audit Report, the DFSI Director of Risk is working with the Better Regulation Governance area and NSW Fair Trading to address the findings specific to NSW Fair Trading from the final Performance Audit.

DFSI has also engaged with NSW Treasury on the key findings and the recommendation will continue to work with NSW Treasury to support improvements in capability and risk culture across the cluster.

Yours sincerely

Martin Hoffman
**Secretary**

6 April 2018

## Response from NSW Police Force

Sensitive: NSW Government

COPY

NSW Police Force

OFFICE OF THE COMMMISSIONER

Ms Margaret Crawford
Auditor-General of NSW
GPO Box 12
SYDNEY NSW 2001

Attention: Ms Claudia Migotto

Your ref: 0006-00163
Our ref: D/2018/212171

Dear Ms Crawford,

I refer to your letter, received 14 March 2018, inviting a NSW Police Force response to the performance audit final report, *Managing risks in the NSW public sector: risk culture and capability*, to be incorporated into the published report.

The NSW Police Force notes that the report identifies steps taken by agencies to strengthen risk culture and remains committed to the NSW Treasury's principles-based approach to risk management and the utilisation of the NSW Treasury's tools and guidance.

The NSW Police Force has introduced a *Risk Assurance Framework*, which explains how each area of the organisation performs under the '3 lines of defence' model. Risk descriptors have been amended to ensure consistency with the report findings.

To ensure key risks to the organisation are identified and communicated to the Executive, along with mitigation strategies, the NSW Police Force has formed a Management Risk Committee.

Building on results of the risk culture survey, the NSW Police Force intends to conduct periodic surveys to further develop the organisation's understanding of its risk culture.

Thank you for the opportunity to review the final report.

Yours sincerely,

**M J Fuller APM**
**Commissioner of Police**

10 APR 2018

Sensitive: NSW Government

Locked Bag 5102 Parramatta NSW 2124 **Tel** 02 8263 6599 En 45599 **Fax** 02 8263 6561 En 45561
**TTY** 02 9211 3776 for the hearing and speech impaired **Web** www.police.nsw.gov.au ABN 43 408 613 180

# Response from NSW Treasury Corporation

NSW Treasury Corporation (TCorp)
Level 22, Governor Phillip Tower
1 Farrer Place, Sydney NSW 2000, Australia
T: +61 2 9325 9325 F: +61 2 9325 9333
W: tcorp.nsw.gov.au ABN: 99 095 235 825

21 March 2018

Margaret Crawford
Auditor-General of NSW
Audit Office of New South Wales
GPO Box 12
SYDNEY NSW 2001

Dear Ms Crawford,

**Managing risks in the NSW Public Sector: Risk Culture and Capability**

Thank you for your letter dated 13 March 2018 and for the opportunity to respond to the Performance Audit Report, "Managing risks in the NSW Public Sector: Risk Culture and Capability".

As the State's provider of financial markets and investment management solutions, effective management of risk is a fundamental requirement for TCorp and a core capability of our broader product and service offering to our clients. TCorp welcomes the contribution from the Audit Office towards strengthening the State's risk management culture and capability, and supports your findings and recommendations.

We look forward to continuing to work with the Audit Office, New South Wales Treasury and other agencies in further embedding a strong risk management culture and capability across the State.

Once again thank you for your report.

Yours sincerely,

David Deverall
Chief Executive

## Response from NSW Treasury

NSW GOVERNMENT | Treasury

Ms Margaret Crawford
Auditor-General of NSW
Level 15
1 Margaret Street
Sydney, NSW 2000

Dear Ms Crawford,

**Performance audit - Managing risks in the NSW public sector: risk culture and capability**

Thank you for the opportunity to comment on your report. Strong risk culture and capabilities are essential to ensuring risk management is effective throughout an organisation and I welcome the Auditor-General's focus on such an important area.

There are direct benefits in strengthening risk management practices in the public sector. Treasury's policies and guidance on risk management are designed to meet the needs of a wide range of government agencies.

This audit has provided valuable input on how the audited agencies have embedded risk management into their organisational cultures. The findings of the report will further inform Treasury's strategy and action plan to support the sector in continuing to improve its practice of risk management.

Attached is a table containing specific comments to the findings in the report for your consideration.

Yours sincerely

**Michael Pratt AM**
**Secretary**

*12 April 2018*

GPO Box 5469, Sydney NSW 2001 ■ Telephone: (02) 9228 4567 ■ www.treasury.nsw.gov.au

NSW GOVERNMENT | Treasury

**Performance audit - Managing risks in the NSW public sector: risk culture and capability**
**Treasury Comments on Audit Report – March 2018**

| Ref. | Treasury Comment |
|---|---|
| Pages 1, 3, 9, 23 | **The report recommends Treasury (a) review the scope of its risk management guidance and (b) identify additional guidance, training or activities to improve risk culture across the NSW public sector by May 2019.**<br><br>Treasury supports the recommendations and will:<br><br>• Undertake a high-level review of the scope of the existing suite of polices, guidance and tools, which is informed by the needs of the sector by May 2019 (a).<br>• Identify any additional guidance and focus on improving the practical implementation of existing guidance. Treasury will partner with icare to support capability building in risk management and culture in the sector. |
| Pages 1, 3, 9, 23 | **The report recommends that Treasury should encourage agency heads to assess current risk culture, identify desirable changes and takes steps to address those changes.**<br><br>Treasury supports this recommendation and therefore:<br><br>• Treasury is committed to work together with departments and agency heads to understand practical challenges in creating a strong risk culture and how to best address these.<br>• Treasury will explore opportunities for an increased role of Audit and Risk Committees in Risk Management.<br>• Treasury will work with the Public Service Commission and agencies to consider adding risk culture aspects to the People Matter Survey questions. |
| Page 24 | **The report finds the interface between the Treasury and agencies on risk management could be improved, and there are several areas within Treasury that have a role in risk management.**<br><br>As a measure to improve the interface and clear communication with the sector Treasury will review and refine the customer interface on risk on its website.<br><br>• Treasury will take actions to clarify the roles and responsibilities of the different actors that define the current risk management landscape in the sector. |
| Page 23 | **The report finds Treasury's role in supervising risk management in the NSW public sector is consistent with a principles-based approach.**<br>Treasury's role is consistent with providing a principles-based framework that supports a devolved model of risk management, which fosters transparency rather than just compliance. Treasury is involved in activities to support risk management in the sector, including:<br>• Requiring attestations from agencies on their compliance with TPP 15-03 *Internal Audit and Risk Management Policy for the NSW Public Sector*<br>• Participating on the sector's Enterprise Risk Management Community of Practice (ERMCP)<br>• Liaising with SunCorp and going forward icare on sector training needs. |

GPO Box 5469, Sydney NSW 2001 ■ Telephone: (02) 9228 4567 ■ www.treasury.nsw.gov.au

# Appendix two – Survey results

## Background

In July and August 2017, the Audit Office conducted a survey across employees in the four auditee agencies (TCorp, NSW Police Force, NSW Fair Trading, and Ministry of Health). There were 418 responses. Of these:

- 141 were people managers
- 253 were non-managers
- 24 preferred not to say.

Results may not add up to 100 per cent due to rounding.

## Survey results

| Question | Agree (%) | Neutral (%) | Disagree (%) |
|---|---|---|---|
| 1. Senior leaders in my agency have communicated that effectively managing risks is a priority | 65.5 | 20 | 14.6 |
| 2. Senior leaders in my agency make clear how much risk people in my work group are permitted to take when making decisions | 44.3 | 28.8 | 26.9 |
| 3. If things go wrong in my work group, I feel safe in calling these out | 69.7 | 12.5 | 17.8 |
| 4. I feel encouraged to identify opportunities and better ways of doing my work | 69.7 | 13.2 | 17.1 |
| 5. I feel comfortable in raising issues and challenging ideas and opinions of others in my work group | 70.6 | 14.7 | 14.7 |
| 6. If I manage risks effectively in my day to day job I get positive recognition in my performance reviews | 43.8 | 34.5 | 21.7 |
| 7. When communicating information within my division, attention is given to both bad and good news | 59.2 | 22.5 | 18.2 |
| 8. People in my work group are encouraged to consider risks and issues prior to starting, and during, significant projects | 62.2 | 23.5 | 14.3 |
| 9. I know where to look for support if I need to escalate a risk or issue | 75.8 | 13 | 11.1 |
| 10. I have a good understanding of the most important risks in my work group and how those risks should be managed | 73.7 | 17.1 | 9.3 |
| 11. I receive adequate training on how to manage risks to people, assets and service delivery to perform my day to day job well | 43.8 | 31.7 | 24.5 |
| 12. Risk management adds value to my organisation | 78.8 | 17.5 | 3.7 |

# 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.

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.

# Appendix four – Performance auditing

## What are performance audits?

Performance audits determine whether an agency is carrying out its activities effectively, and doing so economically and efficiently and in compliance with all relevant laws.

The activities examined by a performance audit may include a government program, all or part of a government agency or consider particular issues which affect the whole public sector. They cannot question the merits of government policy objectives.

The Auditor-General's mandate to undertake performance audits is set out in section 38B of the *Public Finance and Audit Act 1983*.

## Why do we conduct performance audits?

Performance audits provide independent assurance to parliament and the public.

Through their recommendations, performance audits seek to improve the efficiency and effectiveness of government agencies so that the community receives value for money from government services.

Performance audits also focus on assisting accountability processes by holding managers to account for agency performance.

Performance audits are selected at the discretion of the Auditor-General who seeks input from parliamentarians, the public, agencies and Audit Office research.

## How are performance audits selected?

When selecting and scoping topics, we aim to choose topics that reflect the interests of parliament in holding the government to account. Performance audits are selected at the discretion of the Auditor-General based on our own research, suggestions from the public, and consultation with parliamentarians, agency heads and key government stakeholders. Our three-year performance audit program is published on the website and is reviewed annually to ensure it continues to address significant issues of interest to parliament, aligns with government priorities, and reflects contemporary thinking on public sector management. Our program is sufficiently flexible to allow us to respond readily to any emerging issues.

## What happens during the phases of a performance audit?

Performance audits have three key phases: planning, fieldwork and report writing. They can take up to nine months to complete, depending on the audit's scope.

During the planning phase, the audit team develops an understanding of agency activities and defines the objective and scope of the audit.

The planning phase also identifies the audit criteria. These are standards of performance against which the agency or program activities are assessed. Criteria may be based on best practice, government targets, benchmarks or published guidelines.

At the completion of fieldwork, the audit team meets with agency management to discuss all significant matters arising out of the audit. Following this, a draft performance audit report is prepared.

The audit team then meets with agency management to check that facts presented in the draft report are accurate and that recommendations are practical and appropriate.

A final report is then provided to the agency head for comment. The relevant minister and the Treasurer are also provided with a copy of the final report. The report tabled in parliament includes a response from the agency head on the report's conclusion and recommendations. In multiple agency performance audits, there may be responses from more than one agency or from a nominated coordinating agency.

## Do we check to see if recommendations have been implemented?

Following the tabling of the report in parliament, agencies are requested to advise the Audit Office on action taken, or proposed, against each of the report's recommendations. It is usual for agency audit committees to monitor progress with the implementation of recommendations.

In addition, it is the practice of Parliament's Public Accounts Committee (PAC) to conduct reviews or hold inquiries into matters raised in performance audit reports. The reviews and inquiries are usually held 12 months after the report is tabled. These reports are available on the parliamentary website.

## Who audits the auditors?

Our performance audits are subject to internal and external quality reviews against relevant Australian and international standards.

Internal quality control review of each audit ensures compliance with Australian assurance standards. Periodic review by other Audit Offices tests our activities against best practice.

The PAC is also responsible for overseeing the performance of the Audit Office and conducts a review of our operations every four years. The review's report is tabled in parliament and available on its website.

## Who pays for performance audits?

No fee is charged for performance audits. Our performance audit services are funded by the NSW Parliament.

## Further information and copies of reports

For further information, including copies of performance audit reports and a list of audits currently in progress, please see our website www.audit.nsw.gov.au or contact us on 02 9275 7100.

Professional people with purpose

## OUR VISION

Our insights inform and challenge government to improve outcomes for citizens.

## OUR PURPOSE

To help parliament hold government accountable for its use of public resources.

## OUR VALUES

**Purpose** – we have an impact, are accountable, and work as a team.

**People** – we trust and respect others and have a balanced approach to work.

**Professionalism** – we are recognised for our independence and integrity and the value we deliver.

auditoffice
OF NEW SOUTH WALES

audit.nsw.gov.au

Level 15, 1 Margaret Street
Sydney NSW 2000 Australia

PHONE +61 2 9275 7100
FAX +61 2 9275 7200

mail@audit.nsw.gov.au

Office hours: 8.30am-5.00pm,
Monday to Friday.

auditoffice
OF NEW SOUTH WALES

audit.nsw.gov.au