Governance Institute of Australia

T +61 2 9223 5744 **F** +61 2 9232 7174
E info@governanceinstitute.com.au
Level 10, 5 Hunter Street, Sydney NSW 2000
GPO Box 1594, Sydney NSW 2001
W governanceinstitute.com.au

6 February 2015

The Director
Financial and Accounting Policy Branch
Fiscal and Economic Group
NSW Treasury
GPO Box 5469
Sydney NSW 2001

By email: audit&risk@treasury.nsw.gov.au

Dear Director

Internal Audit and Risk Management Policy for the NSW Public Sector

Governance Institute of Australia is the only independent professional association with a sole focus on the practice of governance. We provide the best education and support for practising chartered secretaries, governance advisers and risk managers to drive responsible performance in their organisations.

Our members are all involved in governance, corporate administration, company secretarial practice and compliance within their organisations, including public listed and public unlisted companies, private companies, public sector entities and not-for-profit organisations, with their primary responsibility being the development and implementation of governance frameworks.

Governance Institute of Australia welcomes the opportunity to comment on the *Internal Audit and Risk Management Policy for the NSW Public Sector* (the policy & guidelines paper) and draws upon the experience of our members in providing our response.

Concerns with the application of the draft Policy to state statutory bodies and support for a principles-based approach for such agencies

Our prime concerns with the policy & guidelines paper are that, despite using the language of a principles-based approach, it is highly prescriptive and it does not take account of the diversity in size and circumstance of the entities within the public sector.

While the model set out for the management of audit and risk in the policy & guidelines paper may best fit a large government department (with no board), it is likely to be inappropriate for statutory bodies such as state-owned corporations, which operate under their own legislation and in circumstances significantly different from those of government departments (for example, with a governing board comprising independent non-executive directors.

Guidance from the private sector

We encourage NSW Treasury to adopt the principles-based approach set out in Principles 4 and 7 of the ASX Corporate Governance Council's *Corporate Governance Principles and Recommendations* for state statutory bodies. This model provides them with the flexibility to choose the audit and risk management framework best suited to their needs. That is, it is a model that sets out best practice in governance in relation to audit and risk management, but it provides the organisation with the flexibility to tailor their framework in a manner best suited to their role, history, size and culture.

At present, the policy & guidelines paper assumes that a 'one-size-fits-all' approach is suitable for all entities within the public sector. For example, at present, the policy & guidelines paper

mandates a combined audit and risk management committee of a particular composition, which is likely to be unsuitable for both government departments and statutory bodies. Principle 4, by comparison, recommends that an audit committee be comprised of at least three members, all of whom are non-executive directors and a majority of whom are independent and be chaired by an independent director, but does not mandate a combined audit and risk committee and also recognises that an entity may not have an audit committee at all. For state-owned corporations with a governing board, this model is far more appropriate than the composition mandated in the policy & guidelines paper. It should be noted that the current TPP 09-05 provision 3.1.4 stipulates that the audit and risk committee must have no fewer than three (3) members, and no more than five (5) members, of whom a majority must be independent. Hence this provides the scope and potential for the committee to add value to the organisation and to know the organisation.

We note that a government department without a board could achieve real value from the committee composition mandated in the policy & guidelines paper, that is, independent audit and risk committee members with technical/financial expertise, but that applying this composition model to statutory bodies in the same manner takes no account of their having a board and board subcommittees already in place.

Principle 4 further recommends that in circumstances where an entity does not have an audit committee, it must disclose that fact and also disclose the processes it employs that independently verify and safeguard the integrity of its corporate reporting. This accommodates smaller entities whose board size may preclude the constitution of separate board committees. In such circumstances, for example, the entity can meet the principles set out in Recommendation 4.1 by ensuring that the board meets separately as an audit committee with a separate agenda and minutes, thus ensuring that the board focuses on audit for a period of time.

Effectively managing risk

There is no consensus that a combined audit and risk committee is the best model for all entities. Entities need the flexibility to decide for themselves whether a combined audit and risk committee or separate committees best meet the governance needs of the entity. Risk is core to the business and its sustainability and is the responsibility of the whole board. The focus on risk in the policy & guidelines paper is on financial risk. However, the management of risk is far broader than financial risk alone. In many listed entities, for example, risk management responsibility is spread across all board committees, in recognition that the focus on risk needs to extend beyond financial risk. Committees dealing with workplace health and safety, environmental impacts and remuneration will all have a responsibility to provide oversight of risk management in these areas. Indeed, Principle 7 recommends in Recommendation 7.1 that a listed entity should have a committee or committees to oversee risk in recognition of the need for flexibility in how an entity chooses to manage its risk. Footnote 36 on page 28 of the Corporate Governance principles and Recommendations states that ‘The risk committee(s) could be a stand-alone risk committee, a combined audit and risk committee or a combination of board committees addressing different elements of risk.’ An agency might therefore choose to have a risk management committee with a wider charter for risk which could include coverage of the full gambit of the risks facing the business beyond financial risk.

Some agencies may also wish audit and risk to be performed by separate committees if for no reason other than to minimize the size of the agenda and to have a different and more relevant composition of members.

All strategies and all opportunities worth pursuing involve risks that must be monitored and managed. Risk management in public sector agencies is about both protecting value and creating value for the community. Areas of focus include the nature of risks, how they should be measured and valued, what risk combinations are possible, and most importantly, what risk appetite the entity is willing to tolerate. A committee comprised of only independent members with no knowledge of the business are not best placed to set the risk appetite of the entity or monitor the activities of the entity in relation to how its risks are being managed. It is essential to

any functioning risk management framework that management be involved in setting that framework and attendant strategies, yet the current policy & guidelines paper excludes them.

The mandating of a combined audit and risk committee in the policy & guidelines paper, through its link with internal audit, moreover, creates a poor governance outcome as it represents a conflict of interest where internal audit, which provides an independent review of the operational effectiveness of the entity's risk management framework, may also be responsible for the risk management framework. It is of considerable concern that the body charged with independent review and assurance should also be held responsible for the framework it is charged with monitoring.

The Policy also seeks to mandate the roles of the Chief Audit Executive and the Chief Risk Officer. However, while we agree that both functions must be assigned, how and who is assigned should be a matter for each agency to decide. Most significant statutory bodies and agencies already have people who carry out these tasks but they might be known by different names and be in different sections of the agency. The principle should be that as long as the roles are able to be effectively undertaken, they will not be compromised for their objectivity.

On the matter of the Chief Risk Officer, the policy & guidelines paper goes far beyond any recommendation of best practice in any corporate governance code globally. There is no consensus or research to show that a dedicated Chief Risk Officer is the appropriate model for all entities. Principle 4 not only does not mandate a combined audit and risk committee, but also does not mandate a Chief Risk Officer. Again, the entity requires the flexibility to make a dedicated appointment or delegate the management of risk to the entire management team, and throughout the organisation at all staff levels.

Recommendations

Governance Institute strongly recommends that NSW Treasury:

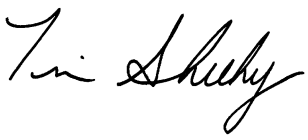
- adopt a different policy & guidelines for state statutory bodies, modelled on the principles-based approach set out in Principles 4 and 7 of the ASX Corporate Governance Council's *Corporate Governance Principles and Recommendations* (see pages 21—23 and 28—30 of the *Corporate Governance Principles and Recommendations*) – the current Policy should be addressed solely to government departments without boards
- ensure that state statutory bodies have the flexibility to adopt the governance model in relation to audit and risk management that best suits the needs of the entity, based on their role, history, size and culture, subject to their explanations in the annual report as to why the model chosen is the best governance model for that entity.

On the matter of ease of compliance, we note that the governance model for audit and risk management is dealt with in Principles 4 and 7 in six pages, compared to the 53 pages of the policy & guidelines paper.

Our detailed comments on the policy & guidelines paper are set out on the following pages.

Governance Institute looks forward to seeing the outcome of the consultation process, and the final Policy which will arise as a result of these discussions. We would welcome the opportunity to discuss any of our views in greater detail.

Yours sincerely



Tim Sheehy
Chief Executive

Specific feedback

1. **Three guiding Principles have been introduced to advise on the intention of the Policy. Do the principles appropriately reflect the outcomes that you would expect agencies should seek from their risk management frameworks, internal audit function and Audit and Risk Committee respectively?**

As noted above, Governance Institute does not support the application of the principles in their present form in the Policy to state statutory bodies. Our members' foremost concern is that it is not appropriate to mandate a 'one-size-fits-all' approach to audit and risk management — mandating an approach is inconsistent with current best practice globally. State statutory bodies require the flexibility to choose the audit and risk management framework best suited to their needs. That flexibility is entirely absent from the current document, which is not principles-based but prescriptive. Governance Institute recommends that NSW Treasury adopt a principles-based approach as set out in Principles 4 and 7 of the ASX Corporate Governance Council's *Corporate Governance Principles and Recommendations* for application to state statutory bodies. This provides an entity with the flexibility, within the parameters of its specific size, culture and requirements, to manage its audit and risk management framework in a manner best suited to its needs while still being accountable to the overarching principles.

Governance Institute believes that the impact of the proposed amendments in the draft Policy are rigid and is likely to have the effect of delivering a complex and unworkable framework for many statutory entities, as the approach mandates a compliance/conformance approach to implementation, rather than a performance approach that is best fit to the needs of the organisation.

Governance Institute also does not support mandating either combined audit and risk committee, a Chief Risk Officer or a Chief Audit Executive for state statutory bodies. Mandating the combined committee may be unsuitable for particular entities and in some cases could result in the financial aspects of risk management being given undue weight at cost to the oversight of all material business risks, potentially jeopardising the survival of the whole entity.

2. **The eight Core Requirements have been designed to achieve the outcomes indicated by the Principles. Are there any significant gaps in the Policy that may undermine the achievement of these outcomes?**

Governance Institute does not support the 'one-size-fits-all' approach set out in the Policy. This approach does not take account of the diversity of size and circumstances of entities within the public sector. The commentary in the Policy undermines the Principles set out in the document.

3. **Nomination of a Chief Risk Officer is encouraged in the draft Policy. Should this role be mandated for some, or all, agencies?**

Governance Institute strongly recommends against mandating a Chief Risk Officer.

Within the risk appetite, framework and process approved by the board of a state statutory body or the head of an agency, risk has to be managed within the business. It is not managed by the board, the audit or risk committee or the risk management unit, but operationally.

Often, an understanding of risk is defined by the responsibilities relating to particular aspects of the business. It is the business strategy that unites the efforts of disparate aspects of the business. In order for an understanding of risk to cascade through the organisation, management teams need to understand the priorities of the organisation, the rationale for

funding certain projects and not others and also the expected results from that prioritisation, including how those results will be measured.

To embed an awareness of risk in the agency it needs to be defined not only as hazards to be avoided, but also as opportunities to be realised and the uncertainties attached to those opportunities. Clarifying this definition throughout the business enables all employees to understand that risk and its management is essential to the growth of the business. In turn, this enables clarity as to who is required to take ownership of particular risks within the entity, with concomitant reporting responsibilities on the management of those risks.

An entity may or may not choose to coordinate the participation of all aspects of the business in risk management and the measures by which identified risks and their treatments will be tracked by establishing a risk management function. Such a function may or may not include a Chief Risk Officer. Given that the particular circumstances and size of the entity should determine how risk management responsibility will be allocated within the entity, it would be a poor governance outcome to mandate a Chief Risk Officer for state statutory bodies.

Furthermore, where a Chief Risk Officer is mandated for government departments without boards, they should not be wholly independent. It is vital that this role is not separated from line management, but the Chief Risk Officer should have a direct reporting line to the committee and not have to report through the agency head.

4. The draft Policy proposes mandating wholly independent Audit and Risk Committees? Would this improve the governance of agencies?

Governance Institute does not support mandating a wholly independent combined Audit and Risk Committee for state statutory bodies. Mandating such combined committees may be appropriate for government departments without boards where the agency head functions as a CEO, but Governance Institute is firmly of the view that it will not improve the governance of state statutory agencies. Rather, it may, in fact, foster poor governance outcomes.

Risk is core to the business and its sustainability and is the responsibility of the whole board, management and all employees. While we agree that the principle of independence should dominate and control the committee, as noted above, excluding all persons who are not independent for eligibility on the Audit and Risk Committee denies the possibility to draw valuable information and expertise from management and/or a non-independent board member. For example, it may be appropriate to have the CEO and/or CFO as a member of the committee but they should not be the chair of the committee. The inclusion of management is particularly relevant in relation to risk management in order to form a depth of understanding of the business or strategic operations of the organisation. Their exclusion will also result in a loss of opportunity for public sector individuals to develop executive leadership skills (especially in governance and oversight). We are not advocating that management should dominate the committee, rather that there should be a requirement for some representation of management on the committee.

We refer again to Principles 4 and 7 of the ASX Corporate Governance Council's *Corporate Governance Principles and Recommendations* which recommend that the audit and risk management committees (which may be combined or separate) have at least three members, all of whom are non-executive directors and a majority of whom are independent and be chaired by an independent director. This is the most appropriate committee composition to be adopted for state statutory bodies.

Governance Institute supports mandating an audit committee, but does not support mandating a combined audit and risk committee for state statutory bodies.

5. **While the minimum term for a Chair of the Audit and Risk Committee has been kept at three years, the maximum term of the Chair has been expanded to five years. A minimum term of three years for a member has been introduced. What are your thoughts on the revised terms for Chairs and members of Audit and Risk Committees?**

Governance Institute can find no rationale in the Policy for the revised terms for chairs and members of the Audit and Risk Committee. We also note that Footnote 17 on page 26 adds further confusion to the proposed revised terms.

Governance Institute does not support the revised terms for chairs and members of the Audit and Risk Committee. We are of the view that the principles that should guide terms for the chair and members of committees are staggered rotation, the independence of the chair and time for each member to gain knowledge of the business and add value.

Our members are of the view that terms for the chair or otherwise should be consistent for all independent members and suggest that they should be three-year appointments with eligibility for a further three-year extension. Appointments should be staggered to ensure consistency and transfer of knowledge, while ensuring rotation. This would promote continuity of knowledge of the agency's business, but avoid the committee becoming stagnant. Governance Institute is also of the view that incoming independent persons often need time to adjust and understand the culture and practice of the business (which are often highly specialised), and thus there is a need to allow adequate time for the member to make a valuable contribution. Our suggested tenure takes this point into consideration.

It may also be administratively burdensome to implement the rotation terms set out in the Policy, particularly in relation to related entity committees, whereas the recommendations set out in the above paragraph align with current best practice and will not be onerous to administer.

6. **Subsequent to finalisation of the Internal Audit and Risk Management Policy, there will be a review of the Guidance on Shared Arrangements and Subcommittees for Audit and Risk Committees (TPP 12-04) early in 2015. What impact, if any, do you think the proposed amendments in the draft Policy should have on the framework in TPP 12-04?**

Governance Institute has no comment to make as to the review of the Guidance on Shared Arrangements and Sub Committees for Audit and Risk Committees and will comment when the draft is released.

General feedback on the proposed amendments

- There are inconsistencies in the draft Policy. For example, it uses the terms 'governing board' and statutory bodies; however, there is no reference to the role of boards in state statutory bodies and it is addressed to the CEOs of government departments. Members found that the term 'agency head', although defined in the definition section, did not assist with understanding that the document is for use by departments and by statutory bodies. The reading of the document by the members and the particular governance problems it causes for state statutory bodies led us to form the view that it is more of a compliance document written for government departments only.
- There is no definition of independence in 'Definitions'.
- Principle 3 of the draft Policy notes that the audit and risk committee has an advisory role, which takes no account of the governing role of boards and their committees in

state statutory bodies. Monitoring of management is a core requirement of audit or risk committees where there is a governing board.

- The draft Policy requires clarification as to the requirement of an Attestation Statement at 3.3. Our members note that it appears as a legislative requirement and as such it should be qualified.
- We note at 3.1.17 and 3.3.21 that there is a concern as to the ultimate power given to the agency head in relation to evaluations of the audit and risk committee. The committee and agency head should jointly undertake the evaluation of the committee. Should this be solely within the agency head's control, there is a governance loophole, as an agency head could 'stack' the committee with non-performers, thus ensuring there was no effective monitoring of management.
- At 3.3.7, we recommend that the more appropriate description of the attendance of the agency head at committee meetings to achieve the desired governance outcome is to state that: 'The Audit and Risk Committee may invite the agency head to attend meetings but will be entitled to 'in-camera' sessions without the agency head being present'. The current wording makes the agency head a de facto member of the audit committee. This also appears again on page 47. As we have recommended that an agency head (CEO) could be a member of a risk management committee in state statutory bodies, the charter of the committee would provide for 'in-camera' sessions of the non-executive, independent committee members.
- The draft Policy advocates that the Chief Audit Executive (CAE) must be an internally designated role, meaning the CAE role cannot be outsourced, even if the internal audit function is outsourced. This is argued for accountability purposes. While we appreciate this argument, we have observed that implementation of this principle in some situations undermines the concept, by having the CAE role allocated as an add-on function to positions that are either imbued with a conflict of interest (such as the CFO, COO or DCS), and/or to individuals who have insufficient knowledge of audit to effectively oversee the function. This makes them a contract administrator only, in effect. The principle should be same for both the CAE and the CFO, as long as their roles are effectively undertaken, there should be no conflict of interest if they are not internally sourced. The Audit Committee can oversee that this is occurring.