Greco (Chief Executive Officer, Zurich Insurance Group). Thanks also to John Drzik (President, Global Risk and Digital, MMC) and Alison Martin (Group Chief Risk Officer, Zurich Insurance Group).

Particular gratitude is due to John Scott (Head of Sustainability Risk, Zurich Insurance Group) and Richard Smith-Bingham (Director of Marsh & McLennan Insights, MMC) for their contributions throughout the planning and drafting of the report.

We are also grateful to our three **Academic Advisers:** the National University of Singapore, the Oxford Martin School at the University of Oxford and the Wharton Risk Management and Decision Processes Center at the University of Pennsylvania.

The report has greatly benefited from the insight and expertise of the members of the *Global Risks Report* **Advisory Board:** Rolf Alter (Hertie School of Governance), Sharan Burrow (International Trade Union Confederation), Winnie Byanyima (Oxfam International), Marie-Valentine Florin (International Risk Governance Council), Al Gore (Generation Investment Management), Howard Kunreuther (Wharton Risk Management and Decision Processes Center), Julian Laird (Oxford Martin School), Pascal Lamy (Jacques Delors Institute), Ursula von der Leyen (Federal Minister of Defence of Germany), Maleeha Lodhi (Ambassador and Permanent Representative of Pakistan to the United Nations), Gary Marchant (Arizona State University), Robert Muggah (Igarapé Institute), Moisés Naím (Carnegie Endowment for International Peace), Jonathan Ostry (International Monetary Fund), Phoon Kok Kwang (National University of Singapore), Daniel Ralph (Cambridge Centre for Risk Studies), Nouriel Roubini (New York University), John Scott (Zurich Insurance Group), Peijun Shi (Beijing Normal University), Richard Smith-Bingham (Marsh & McLennan Companies) and Ngaire Woods (University of Oxford).

*****

We are grateful to the following individuals from our Strategic Partners and Academic Advisors.

Marsh & McLennan Companies: Paul Beswick, Blair Chalmers, John Craig, Lorna Friedman, Laura Gledhill, Jason Groves, Bruce Hamory, Kavitha Hariharan, Wolfram Hedrich, Julian Macey-Dare, Tom Quigley, Maurizio Quintavalle, Michael Schwarz, Wolfgang Seidl, Stephen Szaraz, Charles Whitmore and Alex Wittenberg.

Zurich Insurance Group: Lori Bailey, Francis Bouchard, James Brache, Laura Castellano, Lynne Culberson, Cornelius Froescher, James Gould, David Hilgen, Jack Howell, Annina Humanes, Stefan Kroepfl, Sebastian Lambercy, Manuel Lewin, Jessica McLellan, Guy Miller, Eugenie Molyneux, Wes

Nicholas, Pavel Osipyants, Gregory Renand, Jennifer Schneider, Angel Serna, Michael Szoenyi and Daniela Wedema.

National University of Singapore: Tan Eng Chye and Ho Teck Hua.

Oxford Martin School: Charles Godfray.

Wharton: Jeffrey Czajkowski.

*****

We extend our appreciation to the authors of the two articles in the **Risk Reassessment** section of the report. John D. Graham is a regulatory risk management specialist and currently Dean of Indiana University School of Public and Environmental Affairs. András Tilcsik holds the Canada Research Chair in Strategy, Organizations, and Society at the University of Toronto. Chris Clearfield is the founder of System Logic, a risk and strategy consultancy.

*****

We would like to thank the respondents who completed the **Global Risks Perception Survey.** Thanks also go to the participants in our **Global Risks Workshop** in Geneva on 4 October 2018: Daphné Benayoun (Dalberg Global Development Advisers), Bastian Bergmann (Swiss Federal Institute of Technology Zurich – Risk Center), Walter Bohmayr (Boston Consulting Group), Gabriele Cascone (North Atlantic Treaty Organization), Kate Cooke (WWF International), Thomas Gauthier (Geneva University of Applied Sciences), Winston Griffin (Procter & Gamble), Thomas Inglesby (John Hopkins Center for Health Security), Christian Keller (Barclays), Hichem Khadhraoi (Geneva Call), Quentin Ladetto (Federal Department of Defence, Civil Protection and Sport of Switzerland), Julian Laird (Oxford Martin School), June Lee (International Organisation for Migration), Ian Livsey (The Institute of Risk Management), Esther Lynch (European Trade Union), Phil Lynch (International Service for Human Rights), Nicolas Mueller (Federal Department of Defence, Civil Protection and Sport of Switzerland), Tim Noonan (International Trade Union Confederation), Kenneth Oye (Massachusetts Institute of Technology), Julien Parkhomenko (Global Reporting Initiative), Phoon Kok Kwang (National University of Singapore), Danny Quah (National University of Singapore), Maurizio Quintavalle (Marsh & McLennan), Jean-Marc Rickli (Geneva Centre for Security Policy), Carsten Schrehardt (Federal Ministry of Defence of Germany), John Scott (Zurich Insurance Group), Lutfey Siddiqi (LSE Systemic Risk Centre/ NUS Risks Management Institute), Michael Sparrow (World Climate Research Programme), Jacob van der Blij (GAVI, the Vaccine Alliance), Jos Verbeek (World Bank), Marcy Vigoda (United Nations Office for the Coordination of Humanitarian Affairs), Beatrice Weder di Mauro (Centre for Economic Policy Research), Susan Wilding (CIVICUS: World Alliance for Citizen Participation).

The **Future Shocks** series has again benefitted from the generosity of many people who provided their time and ideas. Special thanks are due to the following individuals and groups, whose suggestions strongly shaped a number of the shocks: Open Secrets (Francesca Bosco, David Gleicher and Bruno Halopeau); City Limits (Thomas Philbeck); Against the Grain (Sean De Cleene, Dan Kaszeta and Philip Shetler-Jones); Digital Panopticon (David Gleicher); and Contested Space (Nikolai Khlystov). Thanks also go to the following for their inputs: Nico Daswani, Anne Marie Engtoft Larsen, Diane Hoskins, Mike Mazarr, Ryan Morhard, Linda Peterhans, Jahda Swanborough and Lauren Uppink. Finally, the participants in the Global Risks Workshop, listed above, made invaluable contributions to this year's Future Shocks series, as did members of the Advisory Board.

In addition to those mentioned above, we extend our thanks to all the following for their time and help: David Aikman, Gauhar Anwar, Marisol Argueta, Evelyn Avila, Silja Baller, Daniela Barat, Paul Beecher, Andrew Berkley, Micael Bermudez, Monika Boerlin, Dominik Breitinger,

Pablo Burkolter, Denise Burnet, Angélique Cado, Beatrice Di Caro, Andrew Caruana Galizia, Gill Cassar, Alice Charles, Martha Chary, Jennifer Clauzure, Arnaud Colin, Gemma Corrigan, Victoria Crawford, Alexander Crueger, Attilio di Battista, Roberto Crotti, Nicholas Davis, Sean Doherty, John Dutton, Makiko Eda, Jaci Eisenberg, Nima Elmi, Malik Faraoun, Emily Farnworth, Cody Feldman, Liam Foran, Brian Gallagher, Thierry Geiger, David Gleicher, Fernando Gomez, Stefan Hall, Wadia Ait Hamza, Mike Hanley, Teresa Hartmann, Alice Hazelton, Audrey Helstroffer, Kiriko Honda, Tom Inglesby, Jennifer Jobin, Jeremy Jurgens, Maroun Kairouz, Nikhil Kamath, Andrej Kirn, Elsie Kanza, Nadège Kehrli, Akanksha Khatri, Nikolai Khlystov, Patrice Kreidi, James Landale, Martina Larkin, Sam Leaky, Joo Ok Lee, John Letzing, Mariah Levin, Elyse Lipman, Silvia Magnoni, Maryne Martinez, Fon Mathuros Chantanayingyong, Viraj Mehta, Stephan Mergenthaler, David Millar, Adrian Monck, Fulvia Montresor, Marie Sophie Müller, Chandran Nair, Alex Nice, Robert Nicholls, Mark O'Mahoney, Vangelis Papakonstantinou, Tania Peters, Ciara Porawski, Vesselina Stefanova Ratcheva, Mel Rogers, Katja Rouru, Eeva Salvik, Richard Samans, Philipp Schroeder, Sarah Shakour, Philip Shetler-Jones, Ahmed Soliman, Paul Smyke, Olivier Schwab, Catherine Simmons, Callie Stinson, Masao Takahashi, Terri Toyota, Jean-François Trinh Tan, Victoria Tuomisto, Peter Vanham, Peter Varnum, Lisa Ventura, Aditi Sara Verghese, Dominic Waughray, Olivier Woeffray, Andrea Wong, Karen Wong, Justin Wood, Nguyen Xuan Thanh, Saemoon Yoon, Kira Youdina, Carida Zafiropoulou-Guignard, and Saadia Zahidi.

Thank you to all those involved in the design and production of this year's report. At the World Economic Forum: Jordynn McKnight and Arturo Rago in particular, as well as Sanskruta Chakravarky, Javier Gesto, Floris Landi, Liam Ó Cathasaigh, Ehiremen Okhiulu and Mara Sandoval. And our external collaborators: Robert Gale, Travis Hensgen and Moritz Stefaner (data visualization); Hope Steele (editing); Patrik Svensson (front cover and Future Shocks artwork); Neil Weinberg (charts and graphics); and Andrew Wright (writing and editing).

And thanks also go to Pierre Saouter for his work on the Global Risks Perception Survey 2018–2019.

WORLD ECONOMIC FORUM

COMMITTED TO IMPROVING THE STATE OF THE WORLD

The World Economic Forum, committed to improving the state of the world, is the International Organization for Public-Private Cooperation.

The Forum engages the foremost political, business and other leaders of society to shape global, regional and industry agendas.

World Economic Forum
91–93 route de la Capite
CH-1223 Cologny/Geneva
Switzerland

Tel.: +41 (0) 22 869 1212
Fax: +41 (0) 22 786 2744

contact@weforum.org
www.weforum.org

RESPONSE TO THE DISCUSSION PAPER

A New Risk Mangement and Internal Audit Framework

Riverina Joint Organisation

Contact:
Julie Briggs
CEO
Riverina Joint Organisation
PO Box 646, Wagga Wagga NSW 2650
Ph: (02) 69 319050 Email: eo@riverinajo.nsw.gov.au
www.riverinajo.nsw.gov.au

A NEW RISK MANAGEMENT AND INTERNAL AUDIT FRAMEWORK for local councils in NSW Response to the Discussion Paper Riverina Joint Organisation

Introduction

This response to the Discussion Paper on A New Risk Management and Internal Audit Framework has been prepared after consultation with the Riverina Joint Organisation's Member Councils. The Riverina Joint Organisation's Member Councils are: Bland, Coolamon, Cootamundra- Gundagai, Greater Hume, Junee, Lockhart and Temora councils as well as Riverina Water and Goldenfields Water County Councils.

Our Members agree with the Minister's assertion that risk is inevitable in any organisation including local councils. Councils across NSW have recognised this, with over 70% already having in place internal audit and risk regimes. Our Members are disappointed that the Discussion Paper has not reviewed the regimes that are already in place, in order to identify the shortcomings that justify the introduction of the very expensive and complex approach proposed in the Discussion Paper.

Further, the Discussion Paper, which details the regulatory requirements and operational Framework, has been prepared with virtually no consultation with the sector. The Minister states that the Framework reflects the "unique needs, structure and resources of NSW Local Government". However, our Members question how the proposed approach will "ensure that councils achieve their strategic objectives in the most efficient, effective and economical manner" given the cumbersome, expensive and resource intensive approach that is being proposed.

Our preliminary costings for the implementation of the proposed Framework, which are attached in **Appendix A** show that the estimated total cost for Medium and Small sized councils will be over $450,000 per annum. The cost falls significantly in a shared arrangement but is still over $170,000 per annum. However, this is based on the assumption that it is feasible for the Chief Audit Executive (CAE) to work for all nine Riverina JO Member Councils and the JO. It is also based on the assumption that the Audit, Risk and Improvement Committee (ARIC) will be able to cover all its work for the Member Councils over 2 days of meetings in a single location and that there are only five ARIC meetings per year. If meetings need to be held in individual LGAs then the travel, accommodation and meeting payments will be considerably higher.

The above costings to do not factor in the additional time burdens on council staff to meet the demands of the CAE and the ARIC for the provision of information and attendance at meetings.

In relation to the application of the regime to the operation of Joint Organisations, our Members agree that the complexity of the regime is disproportionate to the operations of not only the Riverina JO but we would suggest most of the JO operations across NSW. Our Members agree that this regime should not apply to Joint Organisations.

Response to the Key Questions

We note that respondents have been asked to address key questions in relation to the proposal. Our responses to the key questions are below:

Will the proposed internal audit Framework achieve the outcomes sought?
This is a complex, process-driven and expensive approach and given its substantial cost it should achieve the outcomes sought. However, the achievement of the outcomes will undoubtedly divert much needed resources from front-line services and facilities. There is no hard evidence that the process will result in increased efficiencies and savings, consequently our Members believe the cost/benefit does not justify its implementation.

We believe more cost-effective approaches would achieve the same outcomes. If the Office of Local Government had undertaken a review of the existing arrangements in the 70% of councils that already have an audit function in place we are sure that a more affordable approach would have been identified.

What challenges do you see for your council when implementing the proposed Framework?
The cost of the delivery will be a significant challenge for small and medium sized councils.

The significant requirements for appointment to an ARIC will be a major barrier to the effective implementation of the regime and is likely to result in significant cost impositions. Committee members must be prequalified via the NSW Government's Prequalification Scheme. The process requires applicants to meet evaluation criteria including, among other things:

- Extensive senior level experience in governance and management of complex organisations
- Functional knowledge in areas such as risk management, performance management, human resources management, internal and external auditing, financial reporting, accounting, management control Frameworks, financial internal controls, governance or business operations.
- Possession of a relevant professional qualification or membership such as Certified Internal Auditor, Certified Practising Accountant, Certified Practicing Risk Manager, Member of the Australian Institute of Company Directors.
- Must also be able to demonstrate leadership qualities, an ability to communicate complex and sensitive assessments tactfully and sound understanding of governance, accountability, financial reporting, internal audit operations and risk management principles.

Exclusions include current employees of all NSW public sector agencies, in addition the independent committee member cannot:

- be a councillor of any council in Australia, a candidate at the last election of a council or a person who has held office in a council during its previous two terms or be employed (currently or during the last three years) by any council in Australia or have a close personal or business relationship with a councillor or a person who has a senior role in the council;
- be a current service provider to the NSW Audit Office, or have been a service provider during the last three years;
- currently, or within the last three years, provided any material goods or services (including consultancy, legal, internal audit and advisory services) to the council which directly affect subjects or issues considered by the Audit, Risk and Improvement Committee;
- be a substantial shareholder, owner, officer or employee of a company that has a material business, contractual relationship, direct financial interest or material indirect financial interest with the council or a related entity, or have an immediate or close family member who is, which could be perceived to interfere with the individual's ability to act in the best interests of the council; or

- currently or previously have acted as an advocate of a material interest on behalf of the council or a related entity.

The pre-qualification criteria is restrictive and precludes many who would add value to Local Government audit processes by the mere fact that they have contextual knowledge about council policies and practices. For example, a retired local government auditor would be perfectly placed to ask relevant questions about council finances and question the conduct of audits. However, under the pre-qualification guidelines, he or she would be prohibited from consideration by the fact that they had been engaged in the local government sector.

Similarly, persons who are currently serving on Audit Committees for councils would be precluded from serving on an ARIC because of the prohibition on those who had provided goods or services to council in the last 3 years.

While excluding people who had previously served as elected representatives on a council that the ARIC is auditing, is understandable, the total exclusion of any person that has ever served on a council anywhere in Australia makes little practical sense. The Local Government knowledge these people hold would be a valuable asset in assessing and reviewing council operations. The current criteria prohibit current and former councillors from all jurisdictions from seeking pre-qualification, which is "overkill". This means that a person who served on a council in Western Australia is prohibited from being part of an ARIC.

Rural and regional councils are going to struggle to find suitable people to serve on their ARIC and the long list of prohibitions is going to make it almost impossible. This may force councils to choose from a limited pool of metropolitan-based people that have little practical experience or knowledge of the operation of a council in a rural, remote or regional context. In addition, it is likely to increase the costs associated with the operation of the ARIC because of transport and accommodation costs.

Finally, we believe that even in a shared arrangement, councils in rural areas are likely to struggle to find suitably qualified people to fill the CAE position. This position requires a very specific set of skills, and generally those with those skills in regional areas are in high demand. The Framework does facilitate the use of an existing senior staff member in the role however because councils cannot put someone in the position that has previously had carriage of an area that is being audited. The position cannot be out-sourced unless through a shared arrangement. Our Members are very concerned that they will not be able to easily recruit for this specialist position.

Does the proposed Framework include all important elements of effective internal audit and risk Framework?

Given the significant costs and resourcing to be allocated to the Framework our Members believe that the important elements are included.

However, it is not clear how the development of the proposed Risk Management Framework will contribute to the Minister's stated goal of achieving a council's "strategic objectives in the most efficient, effective or economical manner". At a time when there is a lot of focus on stripping away "red tape" to improve efficiency; the complexity, reporting, paperwork, staffing and administration required to deliver the proposed Framework cannot possibly result in the more efficient, effective or economic delivery of a council's strategic objectives.

Taking into account the costs associated with engaging the ARIC, the CAE, the Risk Management Officer and additional administrative staff, the logical outcome, particularly for rural councils will be a reduction in resourcing of front-line services. There is a danger that focusing inward on the

examination of council processes will be at the cost of the on-ground services that residents genuinely value.

We believe that the Framework does not recognise the distinct differences and resource capabilities of rural councils compared to metropolitan councils and State agencies. While there is an opportunity to embark on joint arrangements, this still results in expensive outcomes. It would have been far better if frameworks had been developed that reflected the operational realities of councils across NSW, instead a regime that applies to the City of Sydney applies equally to Coolamon Shire Council.

In relation to the fees proposed for the Chairperson, it appears that the Chair will be paid a flat rate only. If multiple meetings are required, then Chairs who took on the position believing the obligation was for 4 meetings a year, may feel they are not being adequately compensated for the additional work. It may be better to set the fixed fee at a lower level and include a meeting fee on top. If meetings for Joint Arrangements cannot be held in a central location and the ARIC members are required to travel this is likely to increase questions relating to the Chair's remuneration.

Is there anything you don't like about the proposed Framework?

Our Members do not believe that the cost warrants the benefits that will accrue from the adoption of the Framework, particularly for small rural and remote councils. The Framework is too complex and too expensive, the cost of delivery will detract from the delivery of on-ground services and support to the community.

The Minister states in the Foreword that the Framework is "based on international standards and the experience of Australian and NSW government public sector agencies". It is a Framework suited to large complex organisations where the most senior staff have little contact with day-to-day operational staff and where ministerial interactions and reporting do not occur with the same frequency and depth as occurs at monthly council meetings where staff report to councillors on every area of council operations.

The Framework ignores the flatter staffing structures of rural councils where the General Manager interacts with every senior staff member every day and most operational staff on at least a weekly basis. There are already checks and balances in place in these councils because of their proximity to staff, councillors and the community. The councillors are charged with ensuring the council's strategic objectives are delivered efficiently, effectively and economically and they do this at every council meeting that is held.

Our Members are concerned that the Framework fails to recognise the role that councillors play in monitoring the operation of a council. The ARIC's powers are significant and we question how they will complement the role of councillors. Residents elect councillors to, among other things, provide oversight of a council's operations and budgets and they hold them accountable for this at every election. Consequently our members are concerned that there appears to be no effective role for councillors in the operation of the ARIC.

We are concerned that there is no limit on the number of meetings that can be called by the ARIC Chair and that this could result in significant cost imposts on councils who do not appear to be in a position to question the calling of additional meetings. There is nothing in place to control the ARIC once it is established.

The ARIC appears to have complete *carte blanche* to speak to whomever it wants, meet whenever it wants and use whatever council resources it deems necessary, as well as controlling the work of a senior council staff member, the CAE, and by extension whoever is providing support to the CAE. If the council and the ARIC end-up at loggerheads where is the resolution process? Who has precedence, the elected council or the ARIC?

In addition, the role of the CAE could be seen to take precedence over the General Manager. If the CAE demands information or work from a staff member who does the staff member answer to? If there are competing demands on the staff member's time, which there inevitably will be, where is the direction that states that the General Manager is the sole arbiter of what takes priority. The Framework appears to be silent on this issue.

An example of the ARIC taking precedence over the council arises if the council decides to combine the CAE roles with Risk Management Co-ordinator's role. The Framework requires that the ARIC endorse the proposal before the combined role can commence, this requirement undermines the authority of the council as the governing body. It is not an appropriate arrangement, this is a decision that should rest solely with the council, after consultation with the ARIC.

Our Members do not support the proposal that once every four years the ARIC is audited by an external auditor to determine its effectiveness. This is a task that should be undertaken by councillors, or a committee of council. In the proposed Framework councillors have no role; therefore they are independent of the ARIC. Consequently they should be in a position to review the operations of the ARIC in order to determine whether the investment they have made in its operation and all its supporting administrative arrangements have effectively and efficiently delivered outcomes for council.

We are also concerned that ARIC's work appears to be duplicating some of the work already undertaken by the NSW Audit Office. There needs to be a clear delineation of boundaries between ARIC and the Audit Office.

Can you suggest any improvements to the proposed Framework?

The Department should develop a framework that reflects the flatter operational structure of rural councils. The proposed Framework would work for large State agencies where staff are operating in multiple locations and there is minimal day-to-day interaction between the most senior staff and those charged with delivering the agency's core objectives. Having another senior staff member, the CAE, running around the council requesting information from stretched staff on activities that have already been reported to their senior managers (who have then included the information in reports to councillors) is a duplication of oversight that will bring very little in the way of a return to council.

The application of the proposed Framework to Joint Organisations is completely inappropriate. Even in a shared arrangement, the Framework cannot work for a Joint Organisation. As stated above this is a Framework appropriate for a highly complex organisation, which the JOs are not. The imposition of this level of red tape on already stretched JOs will push many to breaking point. An organisation with one full-time staff member and an annual budget of less than $500,000, as is the case with most JOs in NSW, does not require the imposition of a complex internal audit function.

We strongly suggest removing the need for a CAE; this is an expensive new position that will be difficult to fill. The CAE cannot undertake Internal Audit activities on any council operations or services that he/she has held responsibility for in the last 5 years, which means that an existing

senior staff member cannot be moved over to the position on either a full-time or part-time basis. The position cannot be outsourced unless it is in a joint arrangement, and even then, it is likely that the best qualified person would still be drawn from the staff of one of the Member Councils. This would mean that the joint CAE could not have carriage over audits in the council from which he or she was original employed.

It has been suggested that the CAE position and the Risk Management Officer position could be combined, however our Members do not believe this is a feasible approach. The CAE position is clearly a senior management role, while the Risk Management Officer is not; in addition, we believe the skill sets required for each position are completely different.

The criteria that has been established for a position on the ARIC will almost certainly result in regional and rural councils having to recruit from a metropolitan area, this will significantly increase costs associated with travel and accommodation. The criteria for members of ARIC should be amended to allow councillors or staff from councils that have not served on the engaging council to serve on the ARIC. This would ensure that people who actually understood how Local Government works could be appointed to the ARIC. The current Australia-wide ban is completely unnecessary.

The criteria should also permit a person who has not, in the last 18 months, provided goods or services to the engaging council to serve on the ARIC. As it currently stands any accountant, lawyer or other consulting professional that has rendered services to the engaging council in the last 3 years cannot be considered. Given the limited pool of people available in rural areas this will restrict the ability of councils to recruit locally or even regionally.

There is a complete block on anyone that has previously acted as an advocate of a material interest on the behalf of the council or a related entity, again this seems extreme and should be restricted to a period of not more than 18 months. Our Members also believe that councillors from the engaging council should be permitted to serve as voting members on the ARIC. This would increase the transparency of the ARIC and providing independent members outnumber council appointed councillors should not cause any significant issues.

Finally our Members strongly advocate for the Government to consider alternative models of delivery of the audit function. A number of our Members already have audit regimes in place that are cost-effective and are delivering benefits to their councils. We believe that there is a lot that can be learned from these models that would reduce the complexity and cost of what is currently being proposed. We have included an outline of these models at **Appendix B.**

Summary

Our Members agree that it is not appropriate to apply the proposed Framework to the operation of Joint Organisations. The approach is far too complex and unwieldy for the JOs who commonly have only one or two staff members at most. The proposal if implemented will be unaffordable for most Joint Organisations.

In relation to the implementation of the Framework for the JO's Member Councils, our Members agree that it is far too complex and expensive. It fails to recognise the flatter administrative structure that is common to most rural councils, and also fails to recognise the existing level of reporting that occurs between staff and councillors, which minimises risk. The benefits that will be derived from

the new Framework will not justify the costs of delivery. Even if our Member Councils were to share the burden, the costs would still exceed the benefits that are likely to flow from implementation.

The ARIC membership qualifications are far too narrow. The criteria should be reviewed to allow people who have recent experience in Local Government to serve on the ARIC. If the current criteria are approved, then rural and remote councils will be forced to engage people from metropolitan areas to serve on the ARIC who are likely to have had minimal exposure to rural and regional communities and are consequently likely to be less effective in the role. There are unique challenges that councils operating in a rural or remote areas face every day and it is essential that councils have the capacity to appoint people that have an understanding of those challenges.

In addition, engaging metropolitan based members will generate additional costs associated with travel and accommodation, while we appreciate there is an option for teleconferencing for ARIC, we believe in reality this will not occur given the nature of the work the ARIC is undertaking.

Our Members are concerned that the ARIC has far too much power to direct council staff and resources. There are no provisions for the resolution of issues between the ARIC and a council and more concerning the Framework does not acknowledge council as the governing body, ensuring its decision-making takes precedence over the ARIC.

Our Members agree that the same outcomes could have been achieved through the adoption of one of the alternative models that we have outlined in Appendix B. We recognise that the models we have put forward are only a small sample of what 70% of the councils in NSW are already doing. Our Members believe that it was open to the Government to analyse these models of operation particularly in rural and remote councils to develop a framework that was actually affordable and feasible for councils that are not located in a metropolitan location.

Our Members request that the proposed Framework be reviewed with the goal of developing a regime that will deliver benefits that equate to the cost of implementation, particularly for rural and remote councils. Our Members would welcome the opportunity to work with the State Government on the development of a more cost-efficient regime for rural and regional councils.

APPENDIX A

1. Single Council Operation – Estimated Costs

EXPENSE ITEM	COST	Comments
Chief Audit Executive		
Salary	$ 150,000.00	
On-costs	$ 54,000.00	
	$ 204,000.00	
Risk Management Officer		
Salary	$ 90,000.00	
On-costs	$ 32,400.00	
	$ 122,400.00	
Admin Support (PT)		
Salary	$ 40,000.00	
On-costs	$ 14,400.00	
	$ 54,400.00	
Other Costs		
Car	$ 15,000.00	
Phone	$ 2,000.00	
Office Miscellaneous	$ 6,000.00	
Printing etc	$ 5,000.00	
	$ 28,000.00	
TOTAL STAFF COSTS	**$ 408,800.00**	
ARIC Operation: Small Council (4 meetings per year + 1 Special Meeting for Financial Statements)		
Chairman	$ 12,522.00	
Members x 2	$ 12,550.00	
Superannuation	$ 2,381.84	
Travel	$ 6,750.00	5 meetings @$450
Accommodation and Sustainance	$ 3,750.00	5 Meetings x 1 night and 1 day @$250
Meeting costs	$ 1,250.00	5 meetings 2 $250
TOTAL ARIC COSTS	**$ 39,203.84**	
ARIC Operation: Medium Council (4 meetings per year + 1 Special Meeting for Financial Statements)		
Chairman	$ 16,213.00	
Members x 2	$ 16,210.00	
Superannuation	$ 3,080.19	
Travel	$ 6,750.00	5 meetings @$450
Accommodation and Sustainance	$ 3,750.00	5 Meetings x 1 night and 1 day @$250
Meeting costs	$ 1,250.00	5 meetings 2 $250
TOTAL ARIC COSTS	**$ 47,253.19**	
TOTAL COSTS OF PROPOSED FRAMEWORK: SMALL COUNCIL	**$ 448,003.84**	
TOTAL COSTS OF PROPOSED FRAMEWORK: MEDIUM COUNCIL	**$ 456,053.19**	

2. Joint Operation: Estimated Costs

EXPENSE ITEM	COST	Comments
Chief Audit Executive		
Salary	$ 150,000.00	
On-costs	$ 54,000.00	
	$ 204,000.00	
Risk Management Officer internal position in each council		Coucils employ their own RMO
Admin Support (F/T)		
Salary	$ 75,000.00	
On-costs	$ 27,000.00	
	$ 102,000.00	
Other Costs		
Car	$ 20,000.00	Additional Travel
Phone	$ 2,000.00	
Office Miscellaneous	$ 6,000.00	
Printing etc	$ 5,000.00	
Total Other Costs	**$ 33,000.00**	
TOTAL COSTS	**$ 339,000.00**	
ARIC Operation: Joint Arrangement (4 meetings per year + 1 Special Meeting for Financial Statements)		Joint arrangement will require 2 sitting days
Chairman	$ 20,920.00	
Members x 3	$ 62,760.00	Additional Member added due to extra work
Superannuation	$ 7,949.60	
Travel	$ 6,750.00	
Accommodation and Sustainance	$ 7,500.00	Councils meet cost otherwise JO membership fees will rise
Meeting costs	$ 1,250.00	More support required internally so F/T position
TOTAL ARIC COSTS	**$ 107,129.60**	
TOTAL COSTS OF PROPOSED FRAMEWORK: JOINT APPROACH	**$ 446,129.60**	
Shared by 9 Members and JO (but only councils pay)	**$ 49,569.96**	If JO contributes then Membership fees rise to cover it.
Plus Each Council engages a Risk Management Officer	$ 122,400.00	
Cost per Council	**$ 171,969.96**	

APPENDIX B

ALTERNATIVE MODELS FOR THE DELIVERY OF INTERNAL AUDITS

Model One: Internal Audit Alliance

An alliance of six councils have joined together to audit each other, the councils jointly share an Internal Auditor who sits as an independent on each Internal Audit Committee.

The Model has been operating successfully for over 10 years.

Structure

Each council has its own Internal Audit committee and appoints its members according to the adopted Charter or Policy. The Committee is usually comprised of:

- General Manager and a Director level staff member from one of the alliance member councils (independent members)
- two councillors; and
- an external independent auditor (the cost of which is shared across the alliance members).

Each council has adopted its own policy/charter for the Internal Audit Committee. The work of the Internal Auditor is supported by each Alliance council's staff, for example the Manager of Business and Governance or the Manager of Corporate Services.

The Committee meets 4 times a year with each of the alliance members.

Risk Management Framework

Modules or areas of investigation identified by the Internal Audit Alliance are investigated by the Internal Auditor, who then provides a series of recommendations. To date the following areas have been investigated by the Internal Auditor:

- Legislative Compliance,
- Fraud,
- Delegations,
- Policy,
- Payroll and HR,
- Procurement
- Contract Management

The development of a Corporate Risk Register is currently underway and this will identify mitigation strategies and appropriate internal controls throughout the organisation. Risk mitigation controls will be considered during strategic planning and corporate plan development.

Reporting, Monitoring and Evaluation

The Internal Auditor reports to the General Manager in the first instance. Internal Audit reports are presented to the Internal Audit Committee. The Internal Auditor speaks to the reports and responds to queries from the Committee. Management provide feedback and management responses are maintained on the Committee's Status Report.

The Alliance has purchased the Pulse software program to manage the IA function and it has been installed. Monitoring and evaluation of the Internal Audit activities and those of the Committee are recorded in the Status Report

Cost of the Model to the Participating Councils
The model costs each of the participating councils approximately $15,000-$20,000 per annum excluding staff time.

Outcomes achieved through the Process

- Each module or area that has been investigated has resulted in improvements to processes, policy development and the creation of action plans to further manage existing risks.
- The ARIC has heightened the awareness of the importance of risk management throughout the Alliance councils, identified existing gaps and areas of high risk and provided needed incentive to devote resources to the development of a risk management Framework. In an environment where resources are spread thin, risk management is not generally a top priority. The Committee has contributed to incorporating risk management within the regular business of Council.

Best features of the Model

- The Internal Audit Alliance Model currently in place is suited for smaller rural Councils as costs are kept to a minimum and shared across the Alliance.
- The identification and approach to the development of a risk management Framework is structured to accommodate small Councils.
- While each Council within the Alliance is independently evaluated, the opportunity to actively network and share information with Councils of a similar size and risk profile is valuable and should not be underestimated.

Weaknesses of the Model

- This model is reliant on a skilled Internal Auditor with a deep understanding of Local Government as well as effective management by Internal Alliance participants.

Model Two: Internal Audit Committee servicing a Single Council

This model operates within a single council that has made the decision to form an Audit, Risk and Improvement Committee (ARIC) and engaged independent committee members who have senior management experience, preferably in local government, financial skills and experience with internal audit and risk management systems.

The actual audits are undertaken by external providers who audit areas determined by the Committee.

The model has been successfully operating for over 5 years.

Structure
The structure of the ARIC is as follows:

- Independent Chair
- Independent Member (1)

- Two councillors
- Mayor attends in an ex-officio capacity.
- Senior staff attached as observers/advisors

The Director of Corporate and Community Services is responsible for the ARIC and internal audit program in addition to all other aspects of the role. There is no other administrative support available. In addition Council has employed a full-time Risk Management Officer.

Council has adopted a Charter for the operation of the Committee.

Risk Management Framework
Council has adopted a Risk & WHS Management System which consists of a set of program elements which include policies, planning activities, responsibilities, procedures and practices, processes and resources. The System consists of 4 elements:

1. *Key policies and commitment* - clearly stating the direction, intentions and commitment to risk management and continuous improvement.
2. *Planning* – developing a Risk & WHS Plan consistent with Council's objectives.
3. *Implementation* – Council develops the capabilities and support mechanisms necessary
4. *Evaluation and Management Review* – performance is regularly reviewed at both the workplace and corporate levels to continually improve its overall Management System.

Reporting, Monitoring and Evaluation
The external auditor conducts the audit in the areas selected by the ARIC. The completed audit reports are presented to the ARIC.

All recommendations from the internal audit reports are presented to the ARIC and maintained in an Audit Matrix. Progress on implementation of recommendations is updated in the Matrix and reported to ARIC quarterly.

Cost of the Model
The annual budget $27,000 not including staff time, as follows:

ARIC operations including meeting fees:	$ 7,000
Internal Audit Activities:	$20,000

Outcomes achieved through the Process
- Improved efficiency and better governance though the implementation of recommendations emanating from Internal Audit projects.
- Direct cost savings in areas such as IT.
- Improved confidence in financial reporting resulting from an independent assessment being undertaken by ARIC and reported to council in the annual financial statements.

Best features of the Model
- Cost effective and achievable within current budget limitations and resource allocations.
- ARIC membership is providing valuable input into financial management and governance matters.

Weakness of the Model

- Implementation of recommendations from internal audit reviews is often outside current resourcing capabilities leading to increased pressure on staff. This is exacerbated when outstanding internal audit recommendations are highlighted through the external audit process and find their way into the final management letter issued by NSW Audit Office. When that happens, what was an internal matter becomes and external matter under the spotlight of NSW Audit Office resulting in even more pressure to implement something that is simply beyond the capability of the organisation.

Model Three: Internal Audit Committee servicing a County Council

This model operates within a single county council and is similar in operation to Model Two. The council has made the decision to form an Audit, Risk and Improvement Committee (ARIC). The model uses two independent members who have recent and relevant knowledge and experience in local government, accounting or finance, auditing, governance with internal audit and risk management systems.

The actual audits are undertaken by external providers who audit areas determined by the ARIC.

The model has been successfully operating since 2012

Structure

The structure of the ARIC is as follows:

- Two Independent Members
- One councillor

ARIC meetings are attended by:

General Manager
Secretariat Support
Governance and Records' Officer
Manager Corporate Services
Manager Governance and Human Resources
Other management as invited or required by ARIC

General Manager, Corporate Services, Governance and HR units provide support to ARIC and Internal Audit.

The ARIC has a charter which is adopted by Council.

Description of Risk Management Framework

Structure

- Governance and HR unit
- Audit and Risk Committee meets 5 times per year
- Internal Audit (contractor)
- External Audit (State assigned)
- Minimal staff resources allocated to risk management function

Policy and procedures

- Risk Management policy
- Risk Management plan
- Risk Management Action plan (6 monthly review)
- Risk Register (6-month review with Executive Management team) – includes Councils risk criteria and treatment plans
- Minutes of ARIC meetings are tabled at Council meetings following ARIC meeting
- Internal audit work program developed every 5 years with 3 audits per year – contracted. Management response provided monitored and reported

Reporting, Monitoring and Evaluation

The external auditor conducts the audit in the areas selected by the ARIC. The completed audit report is provided to the General Manager for response, there are 3 reports per year.

The internal report is provided to the ARIC for review and to provide feedback to management. The Internal Auditor attends the ARIC meetings. The ARIC reports to Council on progress and the implementation of corrective actions.

The ARIC provides an annual report to the County Council's Board. The ARIC Charter makes provision for Internal Audit function to report annually against agreed KPIs.

An Audit Follow-up Plan is submitted to quarterly meetings. Data is recorded via Word documents and Excel spreadsheets retained on Council's information management system.

Cost of the Model

The annual budget $82,190 as follows:

ARIC Members, 5 meetings per year:	$ 4,015
Three Internal Audits per year:	$23,925
ARIC meetings and internal Auditor Attendance at 5 meetings per year:	$ 4,250
Management Support Costs approx.	$50,000

Outcomes achieved through the Process

Currently practices appear to be effective. Most recommendations from audits have been positively accepted. This has resulted in improvements in practice, governance and compliance. Risks that have been identified by the internal audits have had controls applied to them resulting reduced risks.

External audits have resulted in the provision of an unqualified audit opinion on the annual financial statements

Best features of the Model

- Overall principles are sound
- Enterprise risk management provides more robust application
- Increased community confidence in local government

Weaknesses of the Model

- Excessive internal requirements regarding cost and control with significant human resourcing implications.
- Trying to apply one size fits all across local government
- Rate pegging will not allow for the implementation and operating costs for the IA function.
- Arguably too much power rest with the Chief Audit Officer role

A NEW RISK MANAGEMENT AND INTERNAL AUDIT FRAMEWORK

for local councils in NSW

Discussion paper

September 2019

A NEW RISK MANAGEMENT AND INTERNAL AUDIT FRAMEWORK FOR LOCAL COUNCILS IN NSW – DISCUSSION PAPER

2019

ACCESS TO SERVICES

The Office of Local Government is located at:
Street Address: Levels 1 & 2, 5 O'Keefe Avenue, NOWRA NSW 2541
Postal Address: Locked Bag 3015, Nowra, NSW 2541
Phone: 02 4428 4100
Fax: 02 4428 4199
TTY: 02 4428 4209
Email : olg@olg.nsw.gov.au
Website: www.olg.nsw.gov.au

OFFICE HOURS

Monday to Friday
9.00am to 5.00pm
(Special arrangements may be made if these hours are unsuitable)
All offices are wheelchair accessible.

ALTERNATIVE MEDIA PUBLICATIONS

Special arrangements can be made for our publications to be provided in large print or an alternative media format. If you need this service, please contact Client Services on 02 4428 4100.

DISCLAIMER

While every effort has been made to ensure the accuracy of the information in this publication, the Office of Local Government expressly disclaims any liability to any person in respect of anything done or not done as a result of the contents of the publication or the data provided.

Produced by the NSW Office of Local Government, Department of Planning, Industry and Environment

MINISTER'S FOREWARD

Risk is inevitable in any organisation, including local councils. If a council can identify its risks and how they are caused, a council is more likely to succeed in managing these risks and achieving its community objectives.

Internal audit is a globally accepted mechanism for ensuring that an organisation has good governance and is managing its risks successfully. There has been a steady push over recent years for internal audit to be mandated in the NSW local government sector.

As a first step, in 2008, the government released guidelines to assist councils to establish an internal audit function. These guidelines were updated in 2010. The benefits realised by councils who had introduced internal audit into their business led to calls for internal audit to be made mandatory for every council in NSW.

In 2016, the NSW Government made it a requirement under the *Local Government Act 1993* ('Local Government Act') that each council have an Audit, Risk and Improvement Committee in place. This requirement is likely to take effect from March 2021. Councils are also required to proactively manage any risks they face under the new guiding principles of the Act.

The government has since been working to develop the regulatory framework that will support the operation of these committees, and the establishment of a risk management framework and internal audit function in each council. This discussion paper details the regulatory requirements and operational framework being proposed.

There will be nine core requirements that councils will be required to comply with when establishing their Audit, Risk and Improvement Committee, risk management framework and internal audit function. These requirements are based on international standards and the experience of Australian and NSW Government public sector agencies who have implemented risk management and internal audit. Most importantly, they reflect the unique needs, structure and resources of NSW local government.

Formal risk management and internal audit is a vital part of the NSW Government's plan to ensure that councils achieve their strategic objectives in the most efficient, effective and economical manner. A strong and effective risk management and internal audit framework will result in better services for the community, reduced opportunities for fraud and corruption, increased accountability of councils to their communities and a culture of continuous improvement in councils.

I encourage you to provide your feedback and ideas on the proposed model so we can ensure NSW has in place the most robust and effective risk management and internal audit framework for local government possible.

The Hon Shelley Hancock MP
Minister for Local Government

CONTENTS

BACKGROUND AND PURPOSE

1. Risk

All organisations and governments, including councils, operate in uncertain and changing economic, social, political, legal, business and local environments. Risk is defined as the effect of this uncertainty on an organisation's ability to achieve its goals and objectives, where the effect is the potential for a result that is different to what was expected or planned for[1]. Risks that go so far as to threaten to harm or destroy an object, event or person are known as material risks.

Risk can be positive, negative or both, and can address, create or result in opportunities and threats. Risk is often expressed in terms of an event's consequences and the likelihood of its occurrence. Negative risks can include, for example, unexpected financial loss, project failure, extreme weather events, failure of council policy, and fraud or corruption. Positive risks can include, for example, unexpected favourable publicity, changes to legislation, improved technology, new commercial relationships and business contracts.

Internal controls

Internal controls are any action taken by an organisation to manage and minimise the impacts of negative risks or to promote and harness positive risks to increase the likelihood that the organisation's goals and objectives will be achieved. Internal controls can be:

- preventative – to deter undesirable events from occurring
- detective – to detect and correct undesirable events from happening, or
- directive – to cause or encourage a desirable event to occur.

Internal controls generally fall into two categories:

- hard/formal controls – for example, systems, processes, policies, procedures, management approvals, or
- soft controls – for example, employee capability, organisational culture, ethical behaviour of management and staff.

2. Good governance

Governance can be described as the combination and interconnection of decisions, policies, procedures, processes and structures implemented by an organisation's board/governing body to direct and control the organisation and ensure it functions effectively.

Good governance is a key component of successful organisations. It supports an organisation to ensure its goals and objectives are achieved, its operations are performed successfully, it complies with all necessary legal and other requirements, and it uses its resources responsibly with accountability. It also helps an organisation to promote confidence with stakeholders and adapt and function in changing and uncertain environments.

Good governance is directly linked to an organisation's risk management and compliance frameworks.

[1] Adapted from the definition of risk in AS ISO 31000:2018

The three lines of defence against risk

There are a number of different mechanisms organisations can use to ensure they have good governance and are managing their risks. These governance activities are often referred to as 'the three lines of defence' and are described below in the context of local government. A summary diagram is provided on page 8.

1st line of defence – operational functions implemented by a council to own and manage risk

A council's first line of defence against risk is for council staff to own and manage the risks that occur in their sphere of influence. This means they are given responsibility and held accountable for identifying risks and implementing internal controls (where appropriate).

In practice, this generally sees operational management responsible for identifying and assessing risks that occur in their work area and developing internal controls to manage these risks. This can include guiding the development of council policies and procedures and overseeing the implementation of internal controls by the council staff they supervise. Council staff are responsible for following policies and procedures, implementing other controls and notifying managers when issues arise.

Examples of first line of defence activities could include development assessment processes, operational procedures for technical equipment, maintenance of specific pieces of equipment, cash handling procedures, work health and safety requirements, following project plans etc.

2nd line of defence – management functions implemented by a council to ensure operational functions are managing risks

A council's second line of defence against risk is to ensure that the controls in the first line of defence are properly designed, implemented and operating as intended. Examples of the management frameworks that can be implemented in a council's second line of defence include:

- a risk management framework which identifies known and emerging risks the council faces and controls being implemented to manage these risks (further described in this discussion paper)
- a compliance framework which identifies and monitors council's risk of non-compliance with applicable laws, regulations, contracts and policies, and alerts council to changing compliance requirements
- a financial management framework which identifies and monitors council's financial risks, including financial reporting and external accountability[2]
- a fraud control framework which identifies and manages the risk of the incidence of fraud or corruption and includes prevention and monitoring strategies[3]
- business and performance improvement which identifies and manages any business/performance risks and helps council to improve the efficiency, effectiveness and economy of its operations, for example, information technology and work health and safety, and
- project management which is used to identify and manage project risks, for example, poor project governance, flawed scope definition and insufficient resourcing.

---

[2] Councils are required under the Local Government Act (s 413) to prepare financial reports each year to prescribed standards. These reports must be externally audited, be made available for public inspection (s 418), presented at a council meeting along with the auditor's reports (s 419) and included in council's annual report (s 428).

[3] Councils are required to have a fraud and corruption control plan which includes risk management processes that examine the risk of fraud and corruption both internally and externally across the council. The plan should also include internal controls that seek to minimise fraud and corruption occurring.

Second line of defence activities are generally reported to senior and mid-level management, and can be of interest to the Audit, Risk and Improvement Committee.

3rd line of defence – functions that provide independent external assurance

Council's third line of defence against risk is to receive assurance from an independent body external to the council that its risks are being managed appropriately in the first and second lines of defence. External assurance is designed to provide a council with a level of confidence that its goals and objectives will be achieved within an acceptable level of risk.

Independent external assurance is provided by an Audit, Risk and Improvement Committee, supported by an internal audit function.

External assurance activities are reported to the governing body of the council and the general manager.

Other lines of defence

There are also other lines of defence that sit outside an organisation and provide independent assurance that an organisation has good governance and is managing its risk appropriately.

For councils, these include:

- external audit – an annual independent examination and opinion of council's financial statements which also assesses council's compliance with accounting standards, laws and regulations[4]
- performance audit – an audit of council activities to determine whether the council is carrying out these activities effectively, economically, efficiently and in compliance with all laws. A performance audit can include an individual program or service provided by a group of councils, all or part of an individual council, or issues affecting the sector as a whole[5], and
- regulatory bodies – these set minimum requirements for council's lines of defence, and/or assess the effectiveness of council's governance (for example, the Office of Local Government, NSW Ombudsman, Independent Commission Against Corruption, NSW Parliament).

[4] The Local Government Act (s 415) requires each council to have their annual financial reports externally audited by the NSW Auditor-General (s 422) so that the community and the governing body of the council have access to an independent opinion on their validity. The Auditor-General is to also provide a copy of the Independent Audit Report and the Conduct of the Audit to the Office of Local Government, and report to Parliament on local government sector-wide matters arising from the examination of the financial statements of councils and any other issues the Auditor-General has identified during its audit and the exercise of her other functions (s 421C).

[5] The NSW Auditor-General conducts performance audits of councils under the Local Government Act and reports to the Office of Local Government, the council concerned and the Minister for Local Government any findings, recommendations or concerns that arise from a performance audit (s 421B)

Council's three lines of defence against risk

Other lines of defence: external audit, regulators, other external bodies

3rd line of defence: functions that provide independent external assurance

– reported to governing body and general manager

e.g. Audit, Risk and Improvement Committee, internal audit function

2nd line of defence: management functions implemented by council to ensure operational functions are managing risks

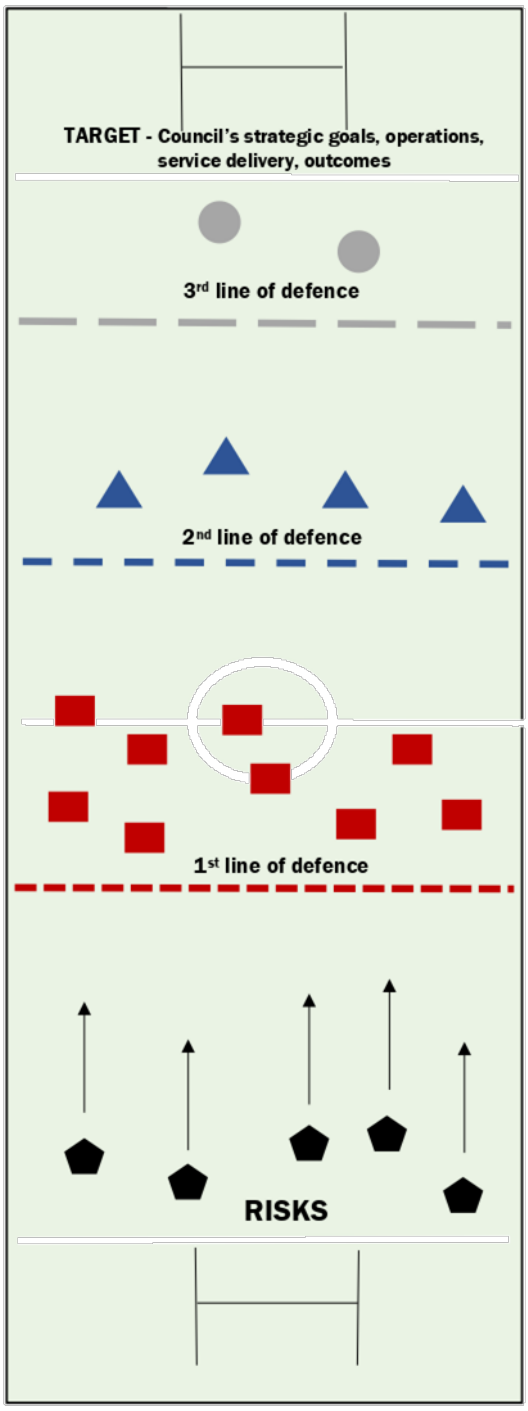
- reported to mid-level/senior management

e.g. risk management framework, regulatory compliance framework, financial management framework, fraud & corruption control framework, business & performance improvement, project management

1st line of defence: operational functions implemented by council to own and manage risk

– conducted by risk owners/managers
– reported to operational management

e.g. identifying risks and implementing controls



3. Purpose of this discussion paper

Amendments made to the Local Government Act in 2016 require each council to be financially sustainable, continuously review its performance, properly exercise its regulatory functions, operate honestly, efficiently and appropriately, and have sound decision-making and risk management practices (s 8A-8C and 223).

They also require each council to establish an Audit, Risk and Improvement Committee as a third line of defence to continuously review and provide independent advice and assurance on council's first and second lines of defence (s 428A). The Local Government Act also envisages the establishment of a risk management framework and internal audit function in each council to support the work of the Committee.

The purpose of this discussion paper is to propose how councils should establish and implement these functions.

It is envisaged that each council's Audit, Risk and Improvement Committee, once established by March 2021, will undertake assurance activities by overseeing each council's internal audit function and risk management framework.

Over time (post-2021), and as resources allow, each council's Audit, Risk and Improvement Committee will be expected to expand its reach to include the other management functions that councils should have in place as part of their second line of defence (for example, financial management, integrated planning and reporting, fraud control, performance etc.).

INTRODUCTION TO RISK MANAGEMENT AND INTERNAL AUDIT

1. Risk management

Risk management describes the coordinated activities an organisation takes to ensure it knows the risks it faces, makes informed decisions about how to respond to these risks, and identifies and harnesses potential opportunities[6].

In practice, it is a deliberate, systematic, comprehensive and documented program that provides a structure to managing risk consistently across the entire organisation, regardless of where, and by who, decisions are made. It also provides a mechanism to shape organisational culture – 'the way we do things around here'.

Risk management is not about being risk averse and it is not a guaranteed way to eliminate all the risks an organisation faces altogether. It is a framework that can help an organisation to reduce its risks to a level that is acceptable and take calculated and appropriate risks that will help it to achieve its strategic goals and deal positively with opportunities.

As required under Australian risk management standards, councils will be required to adopt an 'enterprise risk management' approach under the new regulatory framework.

This will require councils to identify, assess and manage all the risks that affect the ability of the council to meet its goals and objectives, and goes beyond traditional risk management that focuses on insurable risks. Further explanation is provided in the table below.

Traditional risk management	Enterprise risk management
Focuses on insurable risks	Considers all risks that could affect a council's ability to meet its goals, including risks that cannot be insured, for example, a council's reputation
Focused on threats and minimising losses	Considers risks that present both negative and positive consequences or impacts and focuses on adding value
Manages each risk individually and in isolation, often within the particular business unit	Considers risks holistically across the entire council taking into account any connections or interdependencies that could reduce losses or maximize growth opportunities. Risk management is integrated across the entire council
Responses to risk are largely reactive and sporadic	Responses to risk are proactive and continually applied and assessed. Risk management is embedded in organisational culture

[6] Adapted from the definition of risk management in AS ISO 31000:2018

Governing standards

A number of worldwide standards have been developed to help organisations implement risk management. These standards are set by recognised international standards bodies or industry groups and provide an accepted benchmark for risk management practices.

In Australia, the International Organisation for Standardisation's risk management standard *ISO 31000:2009, Risk Management – Guidelines* (AS/NZS ISO 31000:2009) has been accepted as the Australian risk management standard and widely adopted in the private and public sectors. AS/NZS ISO 31000:2009 has just been replaced by AS ISO 31000:2018[7].

AS ISO 31000:2018 states that an organisation's approach to risk management must be based on the following eight specific principles to ensure it is effective:

- risk management is **integrated** into all organisational activities and decision-making processes
- risk management is **structured and comprehensive** process that achieves consistent and comparable results
- the risk management framework and process is **customised** to the organisation
- risk management is **inclusive** of all stakeholders and enables their knowledge, views and perceptions to be considered
- risk management is **dynamic** and able to respond to changes and events in an appropriate and timely manner
- risk management decisions are based on the **best available information** and takes into account any limitations and uncertainties
- risk management takes into account **human and cultural factors**, and
- risk management is continuously and periodically **evaluated and improved** through learning and experience.

To achieve these principles, AS ISO 31000:2018 requires each organisation to ensure its risk management framework includes the following elements:

- **leadership and commitment** – the organisation's board/governing body must clearly communicate and demonstrate strong leadership and commitment to risk management.

  This will be shown by the board/governing body:
  - adopting a risk management policy which communicates the organisation's commitment to risk management and how risk management will be undertaken
  - ensuring the necessary resources are allocated to risk management, and
  - assigning authority and accountability for risk management at appropriate levels in the organisation and aligning risk management to the organisation's objectives
- **integration** – integration of risk management into a council should be a dynamic and iterative process, customised to the organisation's unique needs and culture. Risk management must be made part of the organisation's purpose, governance, leadership, strategy, objectives and operations and everyone in the organisation must understand their responsibility for managing risk.

  This can be achieved through the development and implementation of a risk management plan that provides structure for how the organisation will implement its risk management policy and conduct its risk management activities

[7] More information about AS ISO 31000:2018 can be found at https://www.iso.org/iso-31000-risk-management.html.

- **design** – the organisation's risk management framework must be based on the unique needs, characteristics and risks of the organisation, and its external and internal context.

  This can be achieved by following a tailored risk management process that:
  - evaluates the organisation's internal and external context, operations, stakeholders, complexity, culture, capabilities etc.
  - identifies, assesses and prioritises the risks these present
  - decides how they will be managed
  - allocates resources
  - assigns risk management roles, responsibilities and accountabilities
  - documents and communicates this across the organisation, and
  - demonstrates the organisation's continual commitment to risk management.
- **evaluation** and **improvement** – the organisation must regularly evaluate the effectiveness of its risk management framework and continually adapt and improve how it is designed and integrated throughout the organisation and ensure it is fit for purpose.

2. Internal audit

Internal audit is a mechanism that an organisation can use to receive independent assurance that its first and second lines of defence are appropriate and working effectively. Internal audit can also help an organisation to improve its overall performance.

It does this by:
- providing management with information on the effectiveness of risk management, control and governance processes, and acting as a catalyst for improvement
- providing an independent and unbiased assessment of the organisation's culture, decision-making, financial management, operations, fraud risk, safeguarding of assets, information, policies, processes and systems
- assessing the efficiency, effectiveness, economy and ethical conduct of business activities
- reviewing the achievement of organisational goals and objectives
- assessing compliance with laws, regulation, policies and contracts, and
- looking for better ways the organisation can be doing things.

In relation to risk management, internal audit provides assurance that an organisation's:
- risk management framework is effective and regularly reviewed
- risks are correctly identified and assessed
- risks are being managed to an acceptable level in accordance with the organisation's risk criteria[8], goals and objectives
- internal controls are appropriately designed and effectively implemented, and
- risk information is captured and communicated in a timely manner across the organisation, enabling staff to carry out their risk management responsibilities.

Unlike organisational staff, an internal audit function has no direct involvement in day-to-day operations or financial management of an organisation. It sits within an organisation, but external to it, and investigates how an organisation conducts its day-to-day operations and financial management and helps an organisation to improve those processes and systems.

[8] 'Risk criteria' can also be known as 'risk appetite'

To preserve an internal audit function's independence, it cannot be responsible or held accountable for:

- setting an organisation's risk criteria
- implementing risk management processes
- deciding how an organisation responds to risk, or
- implementing risk responses or controls.

The internal audit function also reports functionally (for internal audit operations) to an organisation's Audit, Risk and Improvement Committee to ensure that it is allowed to operate without inappropriate interference.

Governing standards

The Institute of Internal Auditors (IIA) is the recognised international standard setting body for internal audit and provides professional certification for internal auditors.

The IIA has developed the International Professional Practices Framework (IPPF)[9] which outlines the mandatory requirements for the practice of internal auditing. It describes:

- the definition of internal auditing
- the core principles for the practice of internal auditing
- the international standards for the professional practice of internal auditing, and
- a Code of Ethics which describe the minimum behavioural and conduct requirements of individuals and organisations in the conduct of internal auditing.

These standards are international and are to be applied consistently to the practice of internal audit activity worldwide.

The core components required for internal audit under the IPPF include:

- an **internal audit charter** which communicates internal audit's purpose and authority, its position within the organisation and how internal audit will be undertaken
- reporting arrangements and responsibilities that provide the internal audit function with **independence** from the organisation so that it can be objective and unbiased in its work
- authority for the internal audit function to have **full access** to the records, information, property and personnel it needs to undertake its work
- **work plans** which provide a short-term and long-term structure for the internal audits to be undertaken
- use of **approved methods** and procedures to conduct audits
- a system to **monitor and report** on internal audit findings and the implementation of corrective actions, and
- a **quality assurance and improvement process** to continuously review and improve internal audit activities.

[9] More information about the IPPF can be found at https://www.iia.org.au/technical-resources/professionalGuidance.aspx

Under the IPPF, an effective internal audit function must also exhibit the following 10 mandatory core principles:

- demonstrates integrity
- demonstrates competence and due professional care
- is objective and free from undue influence
- aligns with the strategies, objectives and risks of the organisation
- is appropriately positioned and adequately resourced
- demonstrates quality and continuous improvement
- communicates effectively
- provides risk-based assurance
- is insightful, proactive and future-focused, and
- promotes organisational improvement.

3. Audit Committees

An audit committee is a committee of experts that plays a key role in assisting the board/governing body of an organisation to fulfil its corporate governance and oversight responsibilities. Its main role is to provide advice and assurance regarding:

- the organisation's culture and ethics
- the organisation's first and second lines of defence, including:
  - the effectiveness of risk management and the organisation's internal controls
  - the organisation's fraud and corruption controls
  - business performance and improvement
  - the adequacy of financial management practices and the organisation's accounting, financial records and external reporting
  - systems for managing the organisation's assets
  - compliance with applicable laws, regulations, standards and best practice guidelines, and
- matters that are raised during external and internal audits.

An audit committee also provides a forum for communication between the organisation, senior management, risk and compliance managers, internal auditors and external auditors.

To be effective, an audit committee must be independent from the organisation's management and free from any undue influence.

The size and nature of the committee depends on the industry and size of the organisation. Some organisations establish one committee with responsibility for all these tasks. Larger organisations may establish more than one committee, for example, an audit committee, a risk committee, a compliance committee etc. depending on the nature and extent of the organisation's operations.

There are a number of legal requirements and good practice guides that apply to audit committees depending on the jurisdiction and type of industry and organisation.

4. Use of risk management, internal audit and audit committees in the private and government sectors

Private sector

Audit committees, risk management and internal audit are widely used in the corporate sector worldwide as a mechanism to manage risk and provide independent assurance on governance, controls and financial reporting.

The *Corporations Act 2001* (Commonwealth) requires some Australian companies to ensure that financial reports are true and fair and comply with accounting standards made by the Australian Accounting Standards Board. Most of these companies have audit committees to monitor and oversight their financial reporting (in consultation with external auditors).

The Australian Securities Exchange requires entities included in the S&P/ASX All Ordinaries Index at the beginning of their financial year to have an audit committee during that year[10], and to comply with specific requirements[11] regarding the composition, operation and responsibilities of their audit committee. If an entity does not have an audit committee, this must be disclosed along with the processes the board/governing body employs to independently verify and safeguard the integrity of its corporate reporting.

The establishment of an internal audit function is seen by many investors as essential before they will invest in a company. Since 2014, entities listed on the Australian Securities Exchange have been required to disclose to potential investors whether they have an internal audit function, how the function is structured and what role it performs. If an entity does not have an internal audit function, it must outline why it doesn't, and what assurance arrangements it has in place to manage risk and verify the integrity of financial records[12]. Whilst it is not mandatory, non-listed companies are recommended under Australian standards to have an audit committee as part of good governance[13].

The Australian Prudential Regulation Authority has also mandated the requirement for financial, insurance and superannuation institutions to have internal audit and an audit committee[14]. The audit committee must also meet specific requirements.

Australian Government public sector

While risk management and internal audit is often voluntary in the private sector, many governments around the world have mandated through legislation a requirement for public sector agencies to have an audit committee and some form of risk management.

The Australian Government, under the *Public Governance, Performance and Accountability Act 2013,* requires all Commonwealth entities to establish and maintain appropriate risk management systems and have an audit committee. The *Public Governance, Performance and Accountability Rule 2014* and Commonwealth Risk Management Policy[15] prescribe the requirements for how risk is to be managed.

---

[10] ASX Corporate Governance Council (2016) *ASX Listing Rules* – Rule 12.7

[11] As set out in ASX Corporate Governance Council (2019) *Corporate Governance Principles and Recommendations 4th Edition*

[12] ASX Corporate Governance Council (2014) *Corporate Governance Principles and Recommendations 3rd Edition*

[13] Standards Australia International (2004) *Australian Standard - Good Governance Principles* (AS 8000-2003)

[14] Australian Prudential Regulation Authority (2019) *Prudential Standard CPS 510 Governance (July 2019)*

[15] Australian Government, Department of Finance (2014) *Commonwealth Risk Management Policy*

While an internal audit function is not mandated by legislation, it is recommended that Commonwealth entities establish one to support the audit committee[16] and to ensure that the Secretary or Chief Executive is able to fulfil their other responsibilities under the Act. There have been calls for internal audit to be mandated for Commonwealth entities under the *Public Governance, Performance and Accountability Act 2013*[17].

There are no legislated standards for risk management or internal audit in Commonwealth entities. However, the Australian Government recommends Commonwealth entities conform to ISO risk management standards and the IPPF.

State and Territory public sectors

Most Australian states and territories have mandated risk management, internal audit and/or audit committees in their public sector agencies – these include NSW, Queensland[18], Tasmania[19], Western Australia[20], Victoria[21], and the Northern Territory[22].

In South Australia, only public corporations are required to have an audit committee and an internal audit function[23]. While not mandatory, the Australian Capital Territory recommends its agencies have an audit committee and internal audit function and provides guidance on how they should be established and operate[24].

In NSW, the new *Government Sector Finance Act 2018* requires all NSW Government departments and statutory bodies to have effective systems for risk management, internal control and assurance (including internal audit) that are appropriate for the agency[25].

The NSW Government's Internal Audit and Risk Management Policy[26] further stipulates that all NSW Government departments and statutory bodies are required to establish an Audit and Risk Committee, risk management framework and internal audit function. The core requirements of this policy are modelled on AS ISO 31000:2009[27] and the IPPF. The policy is currently under review by the NSW Government following the release of AS ISO 31000:2018.

---

16 Australian Government, Department of Finance (2018) *Resource Management Guide No. 202. A guide for non-corporate Commonwealth entities on the role of the audit committee* and Australian Government, Department of Finance (2018) *Resource Management Guide No. 202. A guide for corporate Commonwealth entities on the role of the audit committee*

17 IIA (2017) *Submission to the Department of Finance's Review of the Public Governance, Performance and Accountability Act 2013*

18 Section 78 of the *Financial Accountability Act 2009* (QLD) and *Financial and Performance Management Standard 2009* (QLD)

19 *Treasurer's Instruction 108 – Internal Audit* (TAS) September 2011

20 Part 4 of the *Financial Management Act 2006* (WA) and Government of Western Australia, Department of Treasury (2018) *Treasurer's Instructions Part XII – Internal Audit*

21 Victorian Government (2018) *Standing Directions 2018 under the Financial Management Act 1994*

22 *Financial Management Act 1995* (NT) and NT Government (2001) *Treasurer's Directions L4/01– Part 3 Responsible and Accountable Officers, Section 3 Internal Audit* (originally published 1995)

23 Section 31 of the *Public Corporations Act 1993* (SA)

24 ACT Government (2007) *Internal Audit Framework 2007* – this is currently under review by the Act Government and changes may occur during 2019-2020

25 Section 3.6 of the *Government Sector Finance Act 2018*

26 NSW Treasury (2015) *TPP 15-03 Internal Audit and Risk Management Policy for the NSW Public Sector*

27 AS ISO 31000:2018 did not exist when the policy was developed in 2015

Local government

The regulation of audit committees, risk management and internal audit in local councils varies between states and territories. Some jurisdictions, such as South Australia and Tasmania do not explicitly require their councils to have an audit committee, risk management or internal audit function. For those jurisdictions that do require an audit committee and an internal audit function, the approach varies.

All councils in Victoria are legislatively required to have an audit committee[28] and recommended to have an internal audit function that complies with the IPPF[29].

Only large councils in Queensland are legislatively required to have an audit committee[30], but all councils are required to have an internal audit function[31] that complies with the IPPF[32].

The Western Australian Government has legislatively mandated that each council has an audit committee comprising a majority of councillors[33]. A formal internal audit function is not mandated, but encouraged[34].

The experience in NSW is detailed in the next part of this discussion paper.

---

[28] Section 139 of the *Local Government Act 1989 (VIC)*

[29] Local Government Victoria (2011) *Audit Committees, A Guide to Good Practice for Local Government*

[30] Section 105 of the *Local Government Act 2009 (QLD)*

[31] Clause 207 of the *Local Government Regulation 2012 (QLD)*

[32] *Local Government Bulletin 08/15: Internal Audit and Audit Committees*

[33] Part 7 of the *Local Government Act 1995 (WA)* and the *Local Government (Audit) Regulations 1996 (WA)*

[34] Government of Western Australia, Department of Local Government and Communities (2013) *Local Government Operational Guidelines Number 9: Audit in Local Government. The Appointment, Function and Responsibilities of Audit Committees*

PROPOSED RISK MANAGEMENT AND INTERNAL AUDIT FRAMEWORK – THE ROAD AHEAD

1. Risk management and internal audit in NSW local government – the story so far

Local councils in NSW were initially created to provide local communities with basic public services such as water, roads and waste removal on behalf of the NSW Government. As NSW has grown since federation, so too have the responsibilities of local councils. In most local government areas, councils now also provide a wide variety of community services, social infrastructure and local facilities.

NSW councils continue to largely rely on funding from the NSW Government to fulfil their responsibilities, coupled with grants from the Australian Government and rates paid by private citizens. Councils must therefore be accountable to the community and the governments who fund their activities for the way they spend this money and manage public assets.

External independent assurance via an audit committee and internal audit function has been seen for some time as key mechanisms to deliver this accountability. Up to 2008, around 20% of NSW councils were voluntarily following the example set by the private sector and implementing some aspect of external assurance or internal audit function into their operations[35].

In 2008, the Office of Local Government[36] first released guidelines to encourage councils to establish an Audit, Risk and Improvement Committee, risk management framework and internal audit function and set minimum requirements. This led to more councils establishing these mechanisms recognising the benefits they offer.

In 2009, integrated planning and reporting (IP&R) was introduced into the Local Government Act to provide a strategic planning framework for councils. IP&R could also be used to improve the management by councils of actual or potential risks to the strategic goals and objectives.

Reviews by the NSW Auditor-General found that by 2012 over 75 councils had some sort of internal audit function[37], and by 2016 about 60 councils (out of 152 councils), equivalent to 39%, had or shared an Audit, Risk and Improvement Committee[38]. Other research conducted in 2015 suggested full adoption by councils of the other minimum requirements in the Office of Local Government's 2008 Internal Audit Guidelines may have been lower[39].

By June 2018, the NSW Auditor-General[40] found that 86 councils or 62% (out of 138 councils and county councils) now had an internal audit function and the number of councils that had an Audit, Risk and Improvement Committee had risen to 97 or 70%. In terms of risk management, the NSW Auditor-General found that 18 councils did not have a risk management policy and 38 councils did not have a risk register.

---

35 NSW Auditor-General (2012) *NSW Auditor-General's Report - Monitoring local government: Department of Premier and Cabinet, Division of Local Government*

36 Then the Department of Local Government

37 NSW Auditor-General (2012) *NSW Auditor-General's Report - Monitoring local government: Department of Premier and Cabinet, Division of Local Government*

38 Audit Office of NSW (2017) *NSW Auditor-General Update for Audit, Risk and Improvement Committee Chairs*

39 Jones and Beattie (2015) Local Government Internal Audit Compliance, *Australasian Accounting, Business and Finance Journal 9(3)*

40 NSW Auditor-General (2019) *Report on Local Government 2018* (see erratum)

The findings of various public inquiries and corruption investigations since 2008 have led to increased calls for risk management and internal audit to be mandated for NSW councils.

This was realised in 2016 with amendments to the Local Government Act which require councils to establish an Audit, Risk and Improvement Committee by March 2021. These amendments also enable the making of future regulations to mandate a risk management framework and internal audit function in all councils and set a minimum standard of compliance.

This discussion paper outlines what this regulatory framework is proposed to look like.

A timeline of the key influential events that lead to the development of the proposed mandatory framework is provided in **Appendix 1**.

2. Proposed policy framework

The risk management and internal audit framework proposed for the NSW local government sector seeks to:

- ensure each council (including county council/joint organisation) in NSW has an independent Audit, Risk and Improvement Committee that adds value to the council
- ensure each council (including county council/joint organisation) in NSW has a robust risk management framework in place that accurately identifies and mitigates the risks facing the council and its operations
- ensure each council (including county council/joint organisation) in NSW has an effective internal audit function that provides independent assurance that the council is functioning effectively and the internal controls the council has put into place to manage risk are working, and
- establish a minimum standard for these mechanisms based on internationally accepted standards and good practice guidance.

The framework has been based primarily on the NSW public sector risk management and internal audit framework (as recommended by the Independent Commission Against Corruption[41]) and the IPPF[42].

It has also taken into consideration:

- the existing *Internal Audit Guidelines* updated by the Office of Local Government in 2010[43]
- the internal audit-related recommendations of the Independent Local Government Review Panel's 2013 inquiry[44] and the Local Government Acts Taskforce's 2013 review[45]
- recommendations made by the Independent Commission Against Corruption in its various public inquiries into local councils in NSW[46]
- the Australian Government's public sector internal audit framework

---

[41] Independent Commission Against Corruption (2011) *Investigation into the alleged corrupt conduct involving Burwood Council's general manager and others*

[42] The Institute of Internal Auditors (2017) *International Professionals Practices Framework. International Standards for the Professional Practice of Internal Auditing*

[43] Division of Local Government (2010) *Internal Audit Guidelines*

[44] Independent Local Government Review Panel (2013) *Revitalising Local Government. Final Report of the NSW Independent Local Government Review Panel*

[45] Local Government Acts Taskforce (2013) *A New Local Act for New South Wales and Review of the City of Sydney Act 1988*

[46] Independent Commission Against Corruption (2017) *Investigation into the former City of Botany Bay Council Chief Financial Officer and others*. ICAC Report July 2017 and Independent Commission Against Corruption (2011) *Investigation into the alleged corrupt conduct involving Burwood Council's general manager and others*

- opinions, research and recommendations of leaders and practitioners in risk management and internal audit, and
- feedback obtained from NSW Treasury, the NSW Audit Office, the Department of Finance, Services and Innovation, the Institute of Internal Auditors and executive members of the Local Government Internal Auditors Network on earlier drafts of this discussion paper.

An overriding concern has been to ensure that the proposed framework reflects the unique structure and needs of NSW local government and that it also minimises the administrative and resource impacts for councils. For this reason, there are components of the proposed framework that are unique to NSW councils and not reflected in the above-mentioned resources.

3. Proposed statutory framework

The proposed statutory framework regulating internal audit in NSW councils (including county council/joint organisation) will consist of the current provisions in the Local Government Act, new regulations in the Local Government Regulation and new guidelines.

Current legislation

Audit, Risk and Improvement Committee

Section 428A of the Local Government Act (when proclaimed) will require each council to establish an Audit, Risk and Improvement Committee to continuously review and provide independent advice to the general manager and the governing body of the council about:

- whether the council is complying with all necessary legislation
- the adequacy and effectiveness of the council's risk management framework, fraud and corruption prevention activities, financial management processes, and the council's financial position and performance
- the council's governance arrangements
- the achievement of the goals set out in the council's community strategic plan, delivery program, operational plan and other strategies
- how the council delivers local services and how to improve the council's performance of its functions more generally
- the collection of performance measurement data by the council, and
- any other matters prescribed by the Local Government Regulation[47].

Section 428B (when proclaimed) will also allow a council to establish a joint Audit, Risk and Improvement Committee with another council/s including through joint or regional organisations of councils.

Other supporting provisions

Amendments made to the Local Government Act in 2016 to prescribe new guiding principles for councils, and update the prescribed roles and responsibilities of the governing body and general manager will support and inform the work of the Audit, Risk and Improvement Committee and provide for the future establishment of a risk management and internal audit function in each council. These guiding principles and roles and responsibilities have already been proclaimed.

[47] Internal audit will be a matter prescribed under the Regulation.

Guiding principles

The guiding principles of the Local Government Act require each council to carry out its functions in a way that provides the best possible value for residents and ratepayers. The guiding principles also specify that councils are to:

- spend money responsibly and sustainably, and align general revenue and expenses (s 8B(a))
- invest in responsible and sustainable infrastructure for the benefit of the local community (s 8B(b))
- effectively manage their finances and assets and have sound policies and processes for performance management and reporting, asset maintenance and enhancement, funding decisions, and risk management practices (s 8B(c))
- ensure the current generation funds the cost of its services and achieves intergenerational equity (s 8B(d)), and
- manage risks to the local community, area or council effectively and proactively (s 8C(h)).

Role of the governing body

Under section 223, the statutory role and responsibilities of the governing body include:

- directing and controlling the affairs of the council in accordance with the Local Government Act (s 223 (1)(a))
- ensuring as far as possible the financial sustainability of the council (s 223 (1)(c))
- ensuring as far as possible that the council complies with the guiding principles of the Local Government Act (s 223 (1)(d))
- keeping the performance of the council under review (s 223 (1)(g))
- making the decisions necessary to ensure the council properly exercises its regulatory functions (s 223 (1)(h)), and
- being responsible for ensuring that the council acts honestly, efficiently and appropriately (s 223 (1)(l)).

Role of the general manager

Under section 335, the general manager is responsible for ensuring the operational delivery of council's risk management framework and internal audit function. This includes:

- conducting the day-to-day management of the council in accordance with the strategic plans, programs, strategies and policies of the council (s 335(a))
- implementing, without undue delay, the lawful decisions of the council (s 335(b))
- advising the governing body on the development and implementation of the council's plans, programs, strategies and policies (s335(c)), and
- ensuring that the Mayor and other councillors are given timely information and advice and the administrative and professional support necessary to effectively discharge their functions (s335(f)).

Clause 209 of the Local Government Regulation also states that the general manager must ensure that:

- the council complies with all legal financial obligations, including the keeping of accounting records
- effective measures are taken to secure the effective, efficient and economical management of financial operations within each division of the council's administration
- authorised and recorded procedures are established to provide effective control over the council's assets, liabilities, revenue and expenditure and secure the accuracy of the accounting records, and
- lines of authority and the responsibilities of members of the council's staff for related tasks are clearly defined.

New regulations

The operation of sections 428A and 428B will be supported by new regulations. These will prescribe the requirements that councils are to comply with when appointing their Audit, Risk and Improvement Committee and establishing their risk management framework and internal audit function. They will also include internal audit as a function of the Committee under section 428A(2)(i) of the Local Government Act.

The Local Government Regulation will provide for a Model Internal Audit Charter and Model Terms of Reference for Audit, Risk and Improvement Committees which all councils must adopt and comply with. This discussion paper describes the key requirements that will ultimately be prescribed by the Local Government Regulation.

New guidelines

To support compliance with the Local Government Act and Regulation, *Guidelines for NSW Local Government Audit, Risk and Improvement Committees, Risk Management Frameworks and Internal Audit Functions* will be issued under section 23A of the Local Government Act. These Guidelines will outline the core requirements that each council's Audit, Risk and Improvement Committee, risk management framework and internal audit function must have.

A key aim of the Guidelines will be to create a strong and effective risk management framework and internal audit function in all councils by establishing minimum standards that reflect accepted international standards.

The nine core requirements of the Guidelines that councils will need to comply with are summarised below and explained in greater detail throughout the rest of this discussion paper.

The Office of Local Government will, on a periodic basis and at least once every five years, review the Local Government Regulation and Guidelines to assess the efficiency and effectiveness of internal audit requirements and the local government sector's compliance.

CORE REQUIREMENT 1:
Appoint an independent Audit, Risk and Improvement Committee

(a) Each council (including county council/joint organisation) is to have an independent Audit, Risk and Improvement Committee that reviews all the matters prescribed in section 428A of the Local Government Act

(b) The Audit, Risk and Improvement Committee is to operate according to terms of reference, based on a model terms of reference, and approved by the governing body of the council after endorsement by the Committee

(c) The Audit, Risk and Improvement Committee is to comprise of three to five independent members who are prequalified via the NSW Government's *Prequalification Scheme: Audit and Risk Committee Independent Chairs and Members*

(d) Audit, Risk and Improvement Committee members and the Chair are to serve a three to five-year term. A member's term cannot exceed eight years and the Chair's term cannot exceed five years

(e) The Audit, Risk and Improvement Committee is to meet quarterly, with the ability to hold extra meetings if required. A council's general manager and Chief Audit Executive should attend except where excluded by the Committee

(f) Audit, Risk and Improvement Committee members are to comply with council's Code of Conduct and the conduct requirements of the NSW Government's *Prequalification Scheme: Audit and Risk Committee Independent Chairs and Members*

(g) Disputes between the general manager and/or the Chief Audit Executive are to be resolved by the Audit, Risk and Improvement Committee. Disputes with the Committee are to be resolved by the governing body of the council

(h) The Audit, Risk and Improvement Committee is to provide an annual assurance report to the governing body of the council and be assessed by an external party at least once each council term as part of council's quality assurance and improvement program

(i) The general manager is to nominate a council employee/s to provide secretariat support to the Audit, Risk and Improvement Committee. Minutes are to be recorded for all committee meetings

CORE REQUIREMENT 2:
Establish a risk management framework consistent with the current Australian risk management standards

(a) Each council (including county council/joint organisation) is to establish a risk management framework that is consistent with current Australian standards for risk management

(b) The governing body of the council is to ensure that the council is sufficiently resourced to implement an appropriate and effective risk management framework

(c) Each council's risk management framework is to include the implementation of a risk management policy, risk management plan and risk management process. This includes deciding council's risk criteria and how risk that falls outside tolerance levels will be treated

(d) Each council is to fully integrate its risk management framework within all of council's decision-making, operational and integrated planning and reporting processes

(e) Each council is to formally assign responsibilities for risk management to the general manager, senior managers and other council staff and to ensure accountability

(f) Each council is to ensure its risk management framework is regularly monitored and reviewed

(g) The Audit, Risk and Improvement Committee and the council's internal audit function are to provide independent assurance of risk management activities, and

(h) The general manager is to publish in council's annual report an attestation certificate indicating whether the council has complied with the risk management requirements

CORE REQUIREMENT 3:
Establish an internal audit function mandated by an Internal Audit Charter

(a) Each council (including county council/joint organisation) is to establish and internal audit function

(b) The governing body is to ensure that the council's internal audit function is sufficiently resourced to carry out its work

(c) The governing body of the council is to assign administrative responsibility for internal audit to the general manager and to include this in their employment contract and performance reviews

(d) The Chief Audit Executive is to develop an Internal Audit Charter, based on a model charter, which will guide how internal audit is conducted by the council. The Charter is to be approved by the governing body of the council after endorsement by the Audit, Risk and Improvement Committee

CORE REQUIREMENT 4:
Appoint internal audit personnel and establish reporting lines

(a) The general manager is to appoint a Chief Audit Executive to oversee the council's internal audit activities in consultation with the Audit, Risk and Improvement Committee

(b) The Chief Audit Executive is to report functionally to the Audit, Risk and Improvement Committee and administratively to the general manager and attend all committee meetings

(c) The general manager is to ensure that, if required, council has adequate internal audit personnel to support the Chief Audit Executive. Councils will be able to appoint in-house internal audit personnel or completely or partially outsource their internal audit function to an external provider

CORE REQUIREMENT 5:
Develop an agreed internal audit work program

(a) The Chief Audit Executive is to develop a four-year strategic plan to guide the council's longer term internal audits in consultation with the governing body, general manager and senior managers. The strategic plan is to be approved by the Audit, Risk and Improvement Committee

(b) The Chief Audit Executive is to develop an annual risk-based internal audit work plan, based on the strategic plan, to guide council's internal audits each year. The work plan is to be developed in consultation with the governing body, general manager and senior managers and approved by the Audit, Risk and Improvement Committee

(c) The Chief Audit Executive is to ensure performance against the annual and strategic plans can be assessed

CORE REQUIREMENT 6:
How to performing and report internal audits

(a) The Chief Audit Executive is to ensure that the council's internal audits are performed in accordance with the IPPF and current Australian risk management standards (where applicable), and approved by the Audit, Risk and Improvement Committee

(b) The Chief Audit Executive is to develop policies and procedures to guide the operation of the internal audit function, including the performance of internal audits

(c) The Chief Audit Executive is to report internal audit findings and recommendations to the Audit, Risk and Improvement Committee. Each finding is to have a recommended remedial action and a response from the relevant senior manager/s

(d) All internal audit documentation is to remain the property of, and can be accessed by, the audited council, including where internal audit services are performed by an external provider. It can also be accessed by the Audit Risk and Improvement Committee, external auditor and governing body of the council (by resolution)

CORE REQUIREMENT 7:
Undertake ongoing monitoring and reporting

(a) The Audit, Risk and Improvement Committee is to be advised at each quarterly meeting of the internal audits undertaken and progress made implementing corrective actions

(b) The governing body of the council is to be advised after each quarterly meeting of the Audit, Risk and Improvement Committee of the internal audits undertaken and the progress made implementing corrective actions

(c) The Audit, Risk and Improvement Committee can raise any concerns with the governing body of the council at any time through the Chair

CORE REQUIREMENT 8:
Establish a quality assurance and improvement program

(a) The Chief Audit Executive is to establish a quality assurance and improvement program which includes ongoing monitoring and periodic self-assessments, an annual review and strategic external review at least once each council term

(b) The general manager is to publish in the council's annual report an annual attestation certificate indicating whether council has complied with the core requirements for the Audit, Risk and Improvement Committee and the internal audit function

CORE REQUIREMENT 9:
Councils can establish shared internal audit arrangements

(a) A council can share all or part of its internal audit function with another council/s by either establishing an independent shared arrangement with another council/s of its choosing, or utilising an internal audit function established by a joint or regional organisation of councils that is shared by member councils

(b) The core requirements that apply to stand-alone internal audit functions will also apply to shared internal audit functions, with specified exceptions that reflect the unique structure of shared arrangements

(c) The general manager of each council in any shared arrangement must sign a 'Shared Internal Audit Arrangement' that describes the agreed arrangements

Implementation timelines

The transitional arrangements built into the Local Government Act mean that the requirement to have an Audit, Risk and Improvement Committee will not come into force until six months after the next ordinary elections in September 2020. Councils will therefore have until March 2021 to establish their Audit, Risk and Improvement Committees in line with the regulatory requirements proposed in this discussion paper.

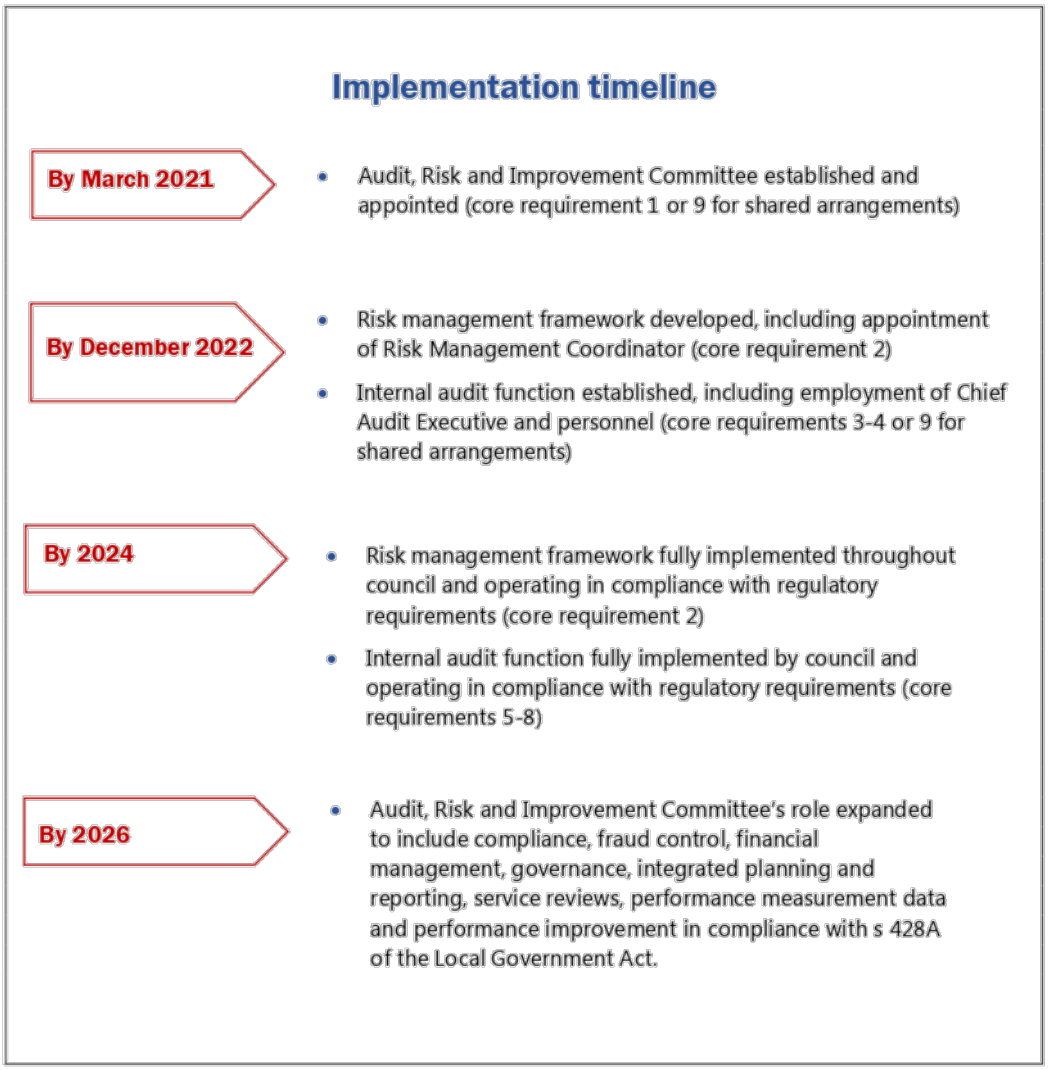
It is proposed that councils will then have a further 18 months, until December 2022, to establish and resource their internal audit function and risk management framework (guided by the Audit, Risk and Improvement Committee).

Councils' Audit, Risk and Improvement Committees will focus on ensuring the council's internal audit function and risk management framework comply with regulatory requirements during the following three years, until 2024.

As these functions are bedded down, the role of the committee is to broaden to comply with the remaining requirements of sections 428A of the Local Government Act.

Full compliance with s 428A of the Local Government Act will be expected by 2026. However, councils that already have an Audit, Risk and Improvement Committee and a mature internal audit function and risk management framework will be encouraged to comply sooner.

This implementation timeline is illustrated below.



4. Benefits of risk management and internal audit for NSW local government

Risk management and internal audit will be a valuable asset for councils.

Risk management will help each council to ensure that any risks to the achievement of its strategic goals and objectives are identified and managed effectively.

Audit, Risk and Improvement Committees and internal audit will provide councils with independent, objective assurance that they are doing things the best way that they can for their community. It will also lead to each council having effective risk management, control and governance processes which will help to instil stakeholder and community confidence in the council's ability to operate effectively.

If implemented effectively, these mechanisms will also lead to each council:

- having better and more efficient levels of service delivery
- achieving better operational consistency across council
- having a greater likelihood of achieving its goals and objectives
- using its resources more efficiently and effectively
- having improved responsiveness and flexibility
- having increased accountability and transparency
- achieving better decision-making and having the confidence to make difficult decisions
- developing good internal governance
- having increased financial stability
- being more resilient to change
- achieving and maintaining compliance with all laws, regulations, internal policies and procedures
- safeguarding its assets
- more reliable, timely and accurate financial and management reporting
- maintaining business continuity, and
- focusing on doing the right things, the right way.

PROPOSED CORE REQUIREMENTS

Core requirement 1: Appoint an independent Audit, Risk and Improvement Committee

Proposal

It is proposed that:

(a) each council (including county council/joint organisation) is to have an independent Audit, Risk and Improvement Committee that reviews all the matters prescribed in section 428A of the Local Government Act

(b) the Audit, Risk and Improvement Committee is to operate according to terms of reference, based on model terms of reference, approved by the governing body of the council after endorsement by the Committee

(c) the Audit, Risk and Improvement Committee is to comprise of three to five independent members who are prequalified via the NSW Government's *Prequalification Scheme: Audit and Risk Committee Independent Chairs and Members*

(d) Audit, Risk and Improvement Committee members and the Chair are to serve a three to five-year term. A member's term cannot exceed eight years and the Chair's term cannot exceed five years

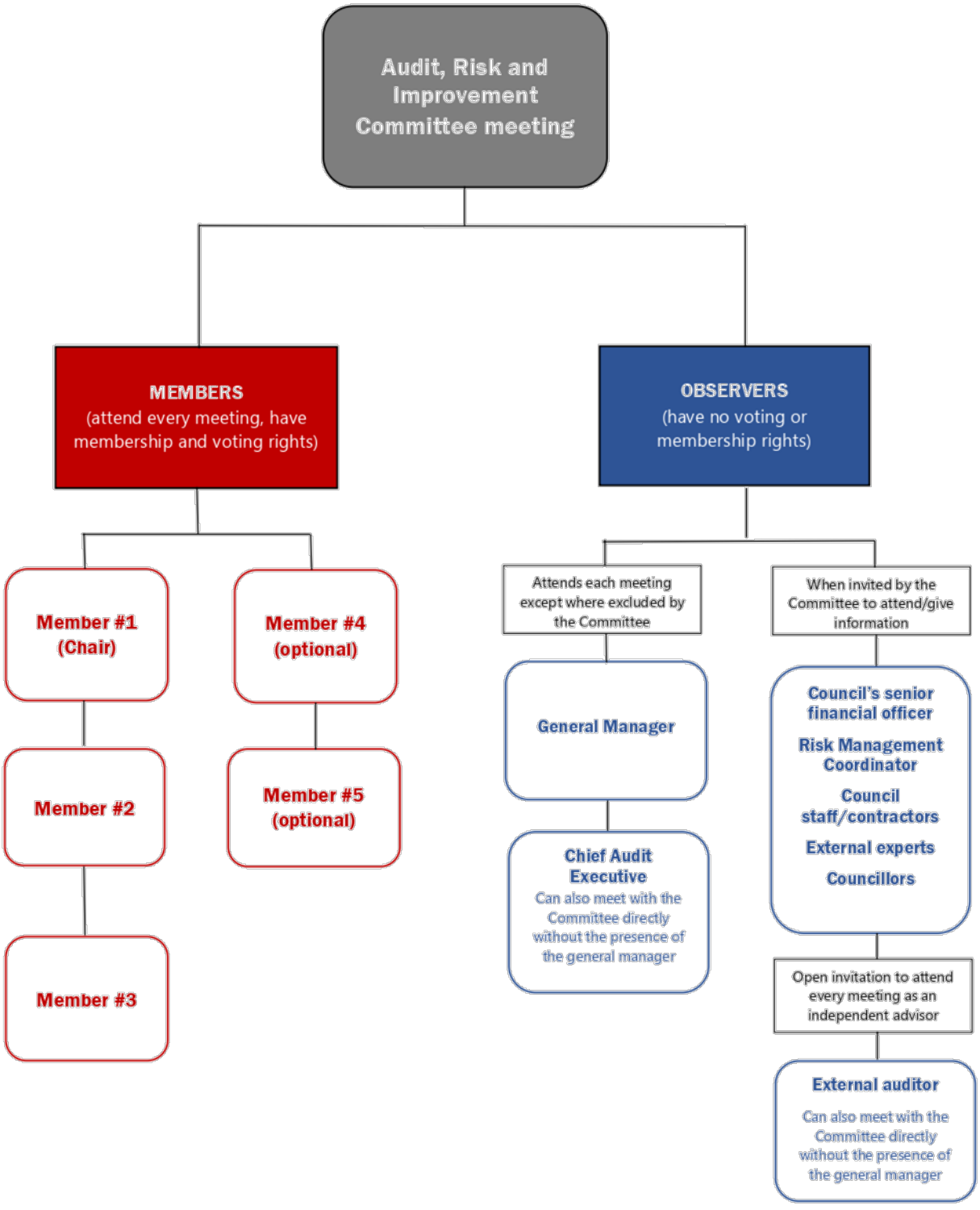
(e) the Audit, Risk and Improvement Committee is to meet quarterly, with the ability to hold extra meetings if required. A council's general manager and Chief Audit Executive should attend except where excluded by the Committee

(f) Audit, Risk and Improvement Committee members are to comply with the council's Code of Conduct and the conduct requirements of the NSW Government's *Prequalification Scheme: Audit and Risk Committee Independent Chairs and Members*

(g) disputes between the general manager and/or the Chief Audit Executive are to be resolved by the Audit, Risk and Improvement Committee. Disputes with the Committee are to be resolved by the governing body of the council

(h) the Audit, Risk and Improvement Committee is to provide an annual assurance review to the governing body of the council and be assessed by an external party at least once each council term as part of the council's quality assurance and improvement program, and

(i) the general manager is to nominate a council employee/s to provide secretariat support to the Audit, Risk and Improvement Committee. Minutes must be recorded for all committee meetings.


Audit, Risk and Improvement Committee meeting
MEMBERS
(attend every meeting, have membership and voting rights)
OBSERVERS
(have no voting or membership rights)
Member #1 (Chair)
Member #2
Member #3
Member #4 (optional)
Member #5 (optional)
Attends each meeting except where excluded by the Committee
General Manager
Chief Audit Executive
Can also meet with the Committee directly without the presence of the general manager
When invited by the Committee to attend/give information
Council's senior financial officer
Risk Management Coordinator
Council staff/contractors
External experts
Councillors
Open invitation to attend every meeting as an independent advisor
External auditor
Can also meet with the Committee directly without the presence of the general manager

Description

(a) Each council (including county council/joint organisation) is to have an independent Audit, Risk and Improvement Committee that reviews all matters prescribed in section 428A of the Local Government Act

Each council in NSW, (including county council/joint organisation), will be required to have an independent Audit, Risk and Improvement Committee that reviews all matters prescribed in section 428A of the Local Government Act.

It is recognised that each council will have different Audit, Risk and Improvement Committee requirements depending on its size, needs, budget and complexity of operations. To provide councils greater flexibility, they can either:

- directly appoint an Audit, Risk and Improvement Committee for their exclusive use
- utilise a joint Committee established by their joint or regional organisation of councils that is shared by member councils, or
- share their Committee with another council/s in close proximity or of their choosing as part of an independent shared arrangement.

It is recommended that county councils, due to their size, enter into a shared arrangement with one of their member councils or utilise an internal audit function established by a joint or regional organisation of councils.

Some of the requirements for shared arrangements will differ from those of stand-alone Audit, Risk and Improvement Committees established for a council's exclusive use (as described in core requirements 1-8). Core requirement 9 outlines the specific requirements of shared arrangements.

Role and functions

Under section 428A of the Local Government Act, each council must have an Audit, Risk and Improvement Committee to keep under review the following aspects of the council's operations:

(a) compliance
(b) risk management
(c) fraud control
(d) financial management
(e) governance
(f) implementation of the strategic plan, delivery program and strategies
(g) service reviews
(h) collection of performance measurement data by the council, and
(i) any other matters prescribed by the regulation (i.e. internal audit).

The Committee will also provide information to the council for the purpose of improving council's performance of its functions.

The Audit, Risk and Improvement Committee is to provide an advisory and assurance role only, and is to have no administrative function, delegated financial responsibility or any management functions.

Audit, Risk and Improvement Committees will be required to give independent advice and assurance to the general manager and the governing body of the council on the issues listed in the following table. It is envisaged that these items will be standing items on agenda of each committee meeting. Beyond this, committees will have the flexibility to address the unique challenges and operating environment of each council.

It will be a matter for each council to decide whether or not it's Audit, Risk and Improvement Committee also serves any entities formed by the council.

Audit, Risk and Improvement Committee: role and responsibilities

Audit

Issue (s 428A)	Committee's role and responsibilities
Internal audit	Advisory: • providing overall strategic and executive direction for internal audit activities • advising the general manager and governing body of the council of the resources necessary to successfully deliver the internal audit function • assessing the adequacy and effectiveness of council's internal audit activities • acting as a forum for communication between the governing body, general manager, senior management, the internal audit function and external audit • overseeing the coordination of audit programs conducted by internal and external audit and other review functions, and • ensuring the council achieves maximum value from its internal audit activities. Review: • the appropriateness of council's Internal Audit Charter, internal audit policies and procedures • audit/risk methodologies used • the findings/recommendations of internal audit activities, particularly recommendations that have been assessed as the most significant according to the risk to the council if they are not implemented • the effectiveness of corrective actions implemented • compliance with statutory requirements • the performance of the Chief Audit Executive and the internal audit function as part of the council's internal audit quality improvement program • the findings of any external reviews of the internal audit function Endorsement of: • the council's Internal Audit Charter, internal audit strategic four-year plan and annual work plan, and • the appointment and remuneration of the Chief Audit Executive
External audit	Advisory: • acting as a forum for communication on external audit issues, and • advising on the findings of external audits and monitoring the implementation by the council of any recommendations for corrective action.

Risk

Issue (s 428A)	Committee's role and responsibilities
Risk management	Advisory – advising whether: • the council has provided sufficient resources for risk management and staff are able to carry out their risk management responsibilities • the council's risk management framework complies with current Australian risk management standards • the council's risk management framework operates effectively and supports the achievement of council's strategic goals and objectives • management has embedded a positive risk management culture • risk management is fully integrated into all aspects of the council, including decision-making processes and operations • risks are formally considered when developing and implementing all council policies, programs, projects and other activities, including procurement • major risks have been identified and assessed by the council and appropriate risk treatments have been implemented that reflect council's risk criteria • risk information is captured and communicated in a timely manner across the council, enabling management and staff to carry out their responsibilities • there are council-specific, fit-for-purpose tools, systems and processes to help all those responsible for managing risk to fulfil their responsibilities, and • the council's risk management policies, procedures and plans are being complied with. Review the appropriateness and effectiveness of the council's: • risk criteria • internal control framework • risk register and risk profile • risk reports • risk management framework in relation to its insurance arrangements, and • business continuity plans and natural disaster plans (including periodic testing). Endorsement of: • the council's risk management policy, risk management plan and risk criteria prior to their approval by the governing body of the council, and • the council's risk profile and risk register/s prior to their approval by the general manager.
Control framework	Providing independent assurance on the following internal controls implemented by the council to manage specific categories of risk: The council's compliance framework - advising whether: • management has embedded a culture which is committed to lawful and ethical behaviour • the council has in place necessary policies and procedures and that these are periodically reviewed and updated • the council is complying with all necessary legislation, regulations, policies and procedures • management has appropriately considered all legal and compliance risks as part of the council's risk assessment and management arrangements • delegations are properly managed and exercised, and • the council's system for monitoring compliance is effective

Issue (s 428A)	Committee's role and responsibilities
	The council's fraud and corruption framework - advising whether the: • council's fraud and corruption prevention plan and activities are adequate and effective, and • council has appropriate processes and systems in place to capture and effectively investigate fraud-related information The council's financial management and external accountability framework – including: • advising whether the council's financial management processes are adequate • assessing the policies and procedures for council management's review and consideration of the council's current and future financial position and performance and the nature of that review (including the approach taken to addressing variances and budget risks) • advising on the adequacy of early close and year-end review procedures, and • reviewing council's financial statements, including: ○ providing input and feedback on council's financial statements ○ advising whether council is meeting its external accountability requirements ○ advising whether appropriate action has been taken in response to audit recommendations and adjustments ○ satisfying itself that the financial statements are supported by appropriate management signoff ○ reviewing the 'Statement by Councillors and Management' (made pursuant to s 413(2)(c) of the Local Government Act) ○ reviewing the processes in place designed to ensure that financial information included in the council's annual report is consistent with the signed financial statements ○ reviewing cash management policies and procedures ○ reviewing policies and procedures for the collection, management and disbursement of grants and tied funding, and ○ satisfying itself that the council has a performance management framework that is linked to organisational objectives and outcomes. The council's governance framework – including: • advising on the adequacy and robustness of the processes and systems that the council has put in place to govern day-to-day activities and decision-making, and • reviewing whether controls over external parties such as contractors and advisors are sound and effective.

Improvement

Issue (s 428A)	Committee's role and responsibilities
Strategic planning	• advising whether the council is achieving the objectives and goals it set out in its community strategic plan and has successfully implemented its delivery program, operational plan and other strategies
Service delivery	• advising how the council is delivering local services and how it could improve its service delivery performance
Performance data and measurement	• assessing the adequacy of the performance indicators and data the council uses to measure its performance

Learning and development program

Some councils, particularly larger metropolitan councils, already have an established risk management and internal audit framework and have been successfully been using these assurance methods for some time. They may just need to make some adjustments to their frameworks to comply with the proposed requirements.

There are other councils that are just starting this journey - for example, they may have appointed an Audit, Risk and Improvement Committee and are now beginning the process of bedding down internal audit and risk management in their councils.

There are also some councils, particularly in rural areas, who do not have any type of internal audit or risk management in place yet, and are starting to think about how this might work for their council.

There is an opportunity for councils to learn from each other's knowledge and experiences, especially during the initial implementation stage.

A sharing and learning program for Audit, Risk and Improvement Committees will be established to facilitate sharing information between committees about how they implement s428A of the Local Government Act and perform the other regulatory requirements placed upon them.

A sharing and learning program for councils (general managers, Chief Audit Executives and/or Risk Management Coordinators) will also be established to facilitate the sharing of information and learning from each other, particularly between councils that have already established a strong internal audit and risk management function and those that are just starting this journey.

The development of these programs will be guided by similar programs established by the Australian Government and bodies such as Chartered Accountants Australia and New Zealand, the Australian Institute of Company Directors and the Actuaries Institute.

(b) The Audit, Risk and Improvement Committee is to operate according to terms of reference, based on model terms of reference, approved by the governing body of the council after endorsement by the Committee

Each Audit, Risk and Improvement Committee is to prepare terms of reference to define how it is structured and how it will operate. The terms of reference are to be approved by the governing body after endorsement by the Committee. The terms of reference can also be used by the council as a benchmarking tool to measure the effectiveness of the committee.

The general manager is to ensure that each member of the Audit, Risk and Improvement Committee, including new appointments, are provided with a copy of the terms of reference and a formal induction.

Each Audit, Risk and Improvement Committee's terms of reference are to comply with Model Terms of Reference[48]. This is consistent with councils being required to adopt policies based on model documents (for example, the Model Code of Conduct and the Model Code of Meeting Practice).

The Model Terms of Reference will require each Audit, Risk and Improvement Committee's terms of reference to:

- set out the committee's objectives, authority, composition, tenure, roles, responsibilities, duties, reporting lines, reporting and administrative arrangements
- be sufficiently detailed to ensure there is no ambiguity, and
- have clear guidance on key aspects of the committee's operations.

The Audit, Risk and Improvement Committee will be able to include additional provisions in its terms of reference as long as they do not conflict with the Model Terms of Reference or the IPPF. This will ensure any matters not contemplated by the Model Terms of Reference are addressed by councils in a robust way that complies with internationally recognised industry standards.

As part of the council's quality assurance and improvement program, where the Audit, Risk and Improvement Committee's Terms of Reference include additional provisions, they are to be reviewed annually by the Audit, Risk and Improvement Committee, and once each council term (i.e. four years) by an external party.

(c) The Audit, Risk and Improvement Committee is to comprise of three to five independent members who are prequalified via the NSW Government's *Prequalification Scheme: Audit and Risk Committee Independent Chairs and Members*

Appointment and size of the Committee

The Audit, Risk and Improvement Committee is to be appointed by the governing body of the council. Councils may find it practical to establish a small committee of councillors and the general manager to conduct the selection process and make appointment recommendations to the larger governing body.

[48] The Model Terms of Reference will be drafted by the Office of Local Government in consultation with councils based on the final internal audit framework developed following consultation on this discussion paper

Each council's Audit, Risk and Improvement Committee is to have no fewer than three members and no more than five members. The Chair is to be counted as a member of the committee. The exact size of the committee is to be determined by the governing body of the council, in consultation with the general manager, taking into account the size and complexity of the council's operations and risk profile.

The Chair of the Audit, Risk and Improvement Committee is to act as the interface between the Committee and the general manager, the Committee and the governing body of council, and the Committee and the Chief Audit Executive.

Independence of members

All Audit, Risk and Improvement Committee members must be independent. To be classified as 'independent', a member must be both:

1. **Free of any relationships that could be perceived to result in bias or a conflict of interest or interfere with their ability to act independently.**

   This means an independent committee member cannot:
   - be a councillor of any council in Australia, a candidate at the last election of a council or a person who has held office in a council during its previous two terms
   - be employed (currently or during the last three years) by any council in Australia
   - have a close personal or business relationship with a councillor or a person who has a senior role in the council
   - be a current service provider to the NSW Audit Office, or have been a service provider during the last three years
   - currently, or within the last three years, provided any material goods or services (including consultancy, legal, internal audit and advisory services) to the council which directly affect subjects or issues considered by the Audit, Risk and Improvement Committee
   - be a substantial shareholder, owner, officer or employee of a company that has a material business, contractual relationship, direct financial interest or material indirect financial interest with the council or a related entity, or have an immediate or close family member who is, which could be perceived to interfere with the individual's ability to act in the best interests of the council
   - currently or previously acted as an advocate of a material interest on behalf of the council or a related entity, or

2. **Selected from the panel of prequalified audit and risk committee independent chairs and members administered by the NSW Government[49].**

   The evaluation criteria for prequalification as a member on the Panel includes[50]:
   - extensive senior level experience in governance and management of complex organisations
   - an ability to read and understand financial statements

[49] The NSW Government's *Prequalification Scheme: Audit and Risk Committee Independent Chairs and Members* streamlines selection processes by providing an impartial third party assessment of independent persons seeking appointment to public sector Audit and Risk Committee positions. Individuals prequalified under the scheme have satisfied key skills, knowledge and experience criteria that ensure they will be able to undertake their role on an audit committee effectively. Further information about the scheme can be found at https://www.procurepoint.nsw.gov.au/scm2421. The scheme's prequalification criteria may be amended to ensure that members who wish to work with local government satisfy the unique needs and requirements of councils.

[50] See the prequalification scheme's conditions at https://tenders.nsw.gov.au/dfs/?event=public.scheme.show&RFTUUID=32C22F9B-DCD8-D61D-59601E7558E2FA26 for more information on the scheme's prequalification criteria. These criteria may be amended in relation to council Audit, Risk and Improvement Committees to ensure that members who wish to work with local government satisfy the unique needs and requirements of councils.

- a capacity to understand the ethical requirements of government (including potential conflicts of interest)
- functional knowledge of areas such as:
  - risk management
  - performance management
  - human resources management
  - internal and external auditing
  - financial reporting
  - accounting
  - management control frameworks
  - financial internal controls
  - governance (including planning, reporting and oversight), or
  - business operations
- a capacity to form independent judgements and willingness to constructively challenge/question management practices and information
- a professional, ethical approach to the exercise of their duties
- the capacity to devote the necessary time and effort to the responsibilities of a member of an Audit, Risk and Improvement Committee, and
- possession of a relevant professional qualification or membership (for example, Certified Internal Auditor, Certified Practising Accountant, Chartered Accountant, Certified Practicing Risk Manager, Graduate Member of the Australian Institute of Company Directors) is desirable.

Chairs must also possess:

- leadership qualities and the ability to promote effective working relationships in complex organisations
- an ability to communicate complex and sensitive assessments in a tactful manner to chief audit executives, senior management, board members and Ministers
- a sound understanding of:
  - the principles of good organisational governance and capacity to understand public sector accountability, including financial reporting
  - the business of the department or statutory body or the environment in which it operates
  - internal audit operations, including selection and review of chief audit executives, and
  - risk management principles.

A person prequalified under the scheme as a 'committee member' can only be appointed as a member of an Audit, Risk and Improvement Committee – they cannot be appointed as the Chair. Similarly, only a person pre-qualified as a 'Chair' can be appointed as the Chair of an Audit, Risk and Improvement Committee.

Satisfying both these criteria will ensure Audit, Risk and Improvement Committee chairs and members are sufficiently skilled and experienced and have no real or perceived conflicts of interest. It is important to note that prequalification does not automatically mean that an individual satisfies the independence requirements listed in criteria 1 above.

Living in a local government area is not, in itself, to be considered as impacting a person's ability to be independent of council.

Both the governing body of the council and the general manager must ensure that adequate procedures are in place to preserve the independence of the Audit, Risk and Improvement Committee Chair and committee members. Likewise, the chair and members must notify the governing body and/or general manager if a real or perceived threat to their independence arises[51].

Knowledge, skills and experience collectively needed on the committee

When selecting individual Audit, Risk and Improvement Committee members, the governing body of the council will be required to ensure that the committee as a collective body has the appropriate mix of skills, knowledge and experience to successfully implement its terms of reference and add value to the council.

At least one member of the Audit, Risk and Improvement Committee should have accounting or financial management experience with an understanding of accounting and auditing standards in a local government context.

Each individual should also have sufficient time to devote to their responsibilities as an Audit, Risk and Improvement Committee member.

Fees paid to members and the Chair

Fees paid to Audit, Risk and Improvement Committee members and the Chair are to be the same as those currently paid under the NSW Government's prequalification scheme, as set out in the table below, subject to any changes to the scheme. Members will be able to serve on Audit, Risk and Improvement Committees on a voluntary basis.

The rates include all reasonable costs incurred by members and the Chair engaged under the scheme excluding subsistence and travel costs if travelling into the Sydney metropolitan area from interstate. Subsistence and travel expenses outside the Sydney metropolitan area and/or where the panel member is from interstate are to be charged at the actual cost, or at the rates specified under the *Crown Employees (Public Service Conditions of Employment) Reviewed Award 2009*, whichever is the lesser.

The method of payment (e.g. payroll, invoice) will be at the discretion of the council.

Council size	Indicator	Chair fee (excluding GST)	Member fee (excluding GST)
Large	Expenditure greater than $400 million	$20,920 per annum	$2,092 per meeting day including preparation time
Medium	Expenditure between $50 million and $400 million	$16,213 per annum	$1,621 per meeting day including preparation time
Small	Expenditure less than $50 million	$12,552 per annum	$1,255 per meeting day including preparation time

[51] As part of their inclusion in the prequalification scheme and prior to their engagement taking effect, chairs and members will be required to provide the council and NSW Government and the details of any other panels they are already on or any other significant appointments within or outside the local government sector (including their nature, duration, payments to the NW Government agency administering the scheme). Currently under the scheme, members are only permitted to be appointed to five separate audit committees in the NSW public sector. This requirement will be updated to also include the NSW local government sector.

(d) Audit, Risk and Improvement Committee members and the Chair are to serve a three to five-year term. A member's term cannot exceed eight years and the Chair's term cannot exceed five years

The initial term of membership of an Audit, Risk and Improvement Committee member on any one Audit, Risk and Improvement Committee will be three to five-years to ensure that the committee maintains a fresh approach. Members can be reappointed or extended for a further term/s but the total period of continuous membership on any one committee will not be able to exceed eight years. This includes any term as Chair of the committee. Individuals who have served an eight-year term (either as a member or Chair) must have a three-year break from serving on the committee before being appointed again.

The terms of appointments will commence on the date the legislation is commenced. This includes for any existing members of Audit, Risk and Improvement Committees already established by councils who will remain members under the new arrangements.

Membership is to be regularly rotated to keep a fresh approach and avoid any perceptions of bias or conflicts of interest. Care is to be taken to ensure that membership renewal dates are staggered so knowledge is not lost to the Audit, Risk and Improvement Committee when members change. Ideally, no more than one member should leave the committee because of rotation in any one year.

Each council is to provide a thorough induction to each of its Audit, Risk and Improvement Committee members.

When approving the reappointment or extension of a membership term on the Audit, Risk and Improvement Committee, the governing body of the council is to consider a formal assessment by the Mayor (in consultation with the general manager) of the member's or Chair's performance on the committee.

The Council may engage an external reviewer to undertake this assessment if they choose. Joint or regional organisations may wish to engage an external reviewer that the mayors of member councils can utilise for this purpose.

The reappointment of members is also to be subject to the individual still meeting the independence and prequalification requirements outlined above.

The governing body can appoint the Chair for one term only for a period of three to five-years. The Chair's term can be extended but any extension must not cause the total term of the Chair to exceed five years.

(e) The Audit, Risk and Improvement Committee is to meet quarterly, with the ability to hold extra meetings if required. A council's general manager and Chief Audit Executive should attend except where excluded by the Committee

The Audit, Risk and Improvement Committee is to meet at least quarterly over the course of each year. A special meeting may be held, if needed, to review the council's financial statements.

Meetings can be held in person, by telephone or videoconference.

The committee is to ensure that its meeting agenda covers all of its responsibilities, as outlined in the committee's terms of reference, and all the items included in council's annual internal audit work plan.

The Audit, Risk and Improvement Committee will also be able to hold additional meetings when significant unexpected issues arise, or the Chair is asked to hold an additional meeting by the majority of committee members, the general manager, or the governing body of the council (by resolution). The Chair will be responsible for deciding if an additional meeting will be held. To enhance accountability, the ability to hold additional meetings is to be documented in the committee's terms of reference.

Any individual Audit, Risk and Improvement Committee member who wishes to meet with the general manager or governing body of the council to discuss internal audit issues is to do so through the Chair of the committee, and vice versa.

Agenda and minutes

The agenda for each Audit, Risk and Improvement Committee meeting is to be circulated at least one week before the meeting. It is to include as standing items all the lines of defence listed in section 428A of the Local Government Act - internal audit, external audit, risk management, compliance, fraud and corruption, financial management, governance, strategic planning, service delivery and performance measurement.

Audit, Risk and Improvement Committee meeting minutes are to:

- include a record of attendance, items of business considered, decisions and actions arising
- be approved by the Chair before circulation
- be provided to the governing body to enable councillors to keep abreast of assurance issues throughout the year, as well as the general manager, Chief Audit Executive and external auditor
- be provided within two weeks of the meeting date to ensure relevant individuals are made aware of any significant issues discussed at the meeting that need to be dealt with, and
- be treated as confidential unless otherwise specified by the committee - public access should be controlled to maintain confidentiality in accordance with council policy.

Quorum

A quorum is to consist of a majority of Audit, Risk and Improvement Committee members. Where the vote is tied, the Chair is to have the casting vote.

Attendance of non-voting observers at committee meetings

Audit, Risk and Improvement Committee meetings will not be open to the public.

In addition to Audit, Risk and Improvement Committee members, the general manager and the Chief Audit Executive are to attend committee meetings as non-voting observers, except where they are excluded by the committee.

The NSW Auditor-General, as council's external auditor, or their representative, is to be invited to each committee meeting as an independent non-voting observer and can choose whether to attend. The committee can also exclude the external auditor if needed.

The Audit, Risk and Improvement Committee will be able to request to meet with any of the following non-voting individuals whenever necessary in order to seek additional information or explanations:

- privately with the Chief Audit Executive and/or external auditor without the general manager present (this is to occur at least annually)
- council's Chief Financial Officer (or equivalent) given their knowledge of, and responsibility for, council's financial management
- council's Risk Management Coordinator
- any councillor (the Chair of the Committee only)
- any employee or contractor of the council, and/or
- any external independent expert or external party whose advice is needed (subject to confidentiality considerations).

These individuals must comply with the Audit, Risk and Improvement Committee's request.

Others may, with the agreement of the Audit, Risk and Improvement Committee, attend as non-voting observers at committee meetings, but such persons will have no membership or voting rights. The committee can also exclude any of these observers from meetings as needed.

The Audit, Risk and Improvement Committee can also request any written reports or other risk management reports from council's senior management, or other related information as necessary, to enable it to fulfil its assurance role in relation to council's risk management framework. The Committee can also request senior managers to present at Committee meetings to discuss their activities and risks.

The committee will be able to hold closed ('in-camera') meetings whenever it needs to discuss confidential or sensitive issues with only committee members of the Audit, Risk and Improvement Committee present.

The Audit, Risk and Improvement Committee can obtain such external legal or other professional or subject matter expert advice, as considered necessary to meet its responsibilities. The service provider and payment of costs for that advice by the council is subject to the prior approval of the governing body of the council.

Access to council, staff, resources and information

The Audit, Risk and Improvement Committee is to have direct and unrestricted access to the general manager, senior management and staff and contractors of the council in order to perform its role.

The Audit, Risk and Improvement Committee is also to have direct and unrestricted access to the council resources and information it needs to perform its role.

The Audit, Risk and Improvement Committee may only release council information to external parties with the approval of the general manager. The general manager's approval is not required where the information is being provided to an external investigative, audit or oversight agency such as, but not limited to, the Office of Local Government, the NSW Audit Office, the Independent Commission Against Corruption or the NSW Ombudsman for the purpose of informing that agency of a matter that may warrant its attention.

(f) Audit, Risk and Improvement Committee members are to comply with the council's Code of Conduct and the conduct requirements of the NSW Government's *Prequalification Scheme: Audit and Risk Committee Independent Chairs and Members*

Under section 440 of the Local Government Act, independent Audit, Risk and Improvement Committee members are subject to and required to comply with the council's Code of Conduct. Complaints or breaches of council's code of conduct will be dealt with in accordance with the *Procedures for the Administration of the Model Code of Conduct for Local Councils in NSW*[52]. Committee members should also be deemed to be a 'designated person' and required to complete and submit returns of interests.

As required under the Model Code of Conduct, Audit, Risk and Improvement Committee members must declare any pecuniary or significant non-pecuniary conflicts of interest at the start of each Committee meeting, before discussion of the relevant agenda item or issue, or when the issue arises. Details of any conflicts of interest should also be appropriately minuted.

Where Audit, Risk and Improvement Committee members or observers at Committee meetings are deemed to have a real or perceived conflict of interest they are to remove themselves from Committee deliberations on the issue.

Given they will have been selected from the NSW Government's panel of prequalified Audit and Risk Committee Independent Chairs and Members, members will also be required to comply with that scheme's conduct requirements[53].

(g) Disputes between the general manager and/or Chief Audit Executive are to be resolved by the Audit, Risk and Improvement Committee. Disputes with the Committee are to be resolved by the governing body of the council

Members of the Audit, Risk and Improvement Committee should maintain an effective working relationship and try to resolve any differences they may have via open negotiation.

However, in the event of a disagreement between the council management and the Chief Audit Executive (for example, about findings or recommendations of audits), it is to be resolved by the Audit, Risk and Improvement Committee. Disputes between the council management and the Audit, Risk and Improvement Committee are to be resolved by the governing body.

Unresolved disputes regarding compliance with statutory or other requirements are to be referred to the Office of Local Government in writing for its resolution.

---

[52] The Procedures can be found at http://www.olg.nsw.gov.au/sites/default/files/Procedures-for-Administration-of-Model-Code-of-Conduct.pdf

[53] The prequalification scheme's code of conduct can be found at https://www.procurepoint.nsw.gov.au/scm2421

(h) The Audit, Risk and Improvement Committee is to provide an annual assurance report to the governing body of the council and be assessed by an external party at least once each council term as part of the council's quality assurance and improvement program

Annual assurance report

As part of council's quality assurance and improvement program, the Audit, Risk and Improvement Committee is to provide an annual assurance report to the governing body which provides:

- a summary of the work the committee performed to discharge its responsibilities during the preceding year
- advice on the appropriateness of the Committee's terms of reference (where the Committee's terms of reference contain additional clauses to those contained in the Model Terms of Reference)
- an overall assessment of the following aspects of council's operations in accordance with section 428A of the Local Government Act:
  - compliance
  - risk management
  - fraud control
  - financial management
  - governance
  - implementation of the strategic plan, delivery program and strategies
  - service reviews
  - collection of performance measurement data by the council, and
  - any other matters prescribed by the regulation (i.e. internal audit), and
- any other information to help the council improve the performance of its functions.

This will ensure that the governing body of the council receives the committee's independent views about these matters in accordance with legislative requirements each year. It will also enable the governing body to assess the work of the Committee each year.

Strategic external review

At least once each council term (i.e. four years) an external strategic review of the effectiveness of the Audit, Risk and Improvement Committee is to be conducted to assess how the committee is functioning. This will provide accountability and ensure that the governing body of the council can assess how the committee's performance and whether any changes to the committee's terms of reference or membership are required.

This strategic external review is to consider:

- whether the Committee has fulfilled its terms of reference
- the appropriateness of the Committee's terms of reference (where the Committee's terms of reference contain additional provisions to those contained in the Model Terms of Reference)
- the performance of Committee members and whether any change of membership is required
- the way the Committee, external auditor, council and internal audit function work together to manage risk and support the council and how effective this is, and
- whether the work of the Committee has contributed to the improvement of the factors identified in section 428A of the Local Government Act.

The external review is to address the collective performance of the Audit, Risk and Improvement Committee, as well as the individual performance of each member and the Chair. In considering the outcomes of the external strategic review, the review is to consider feedback on each member's performance by the Chair of the Committee, mayor and general manager. The governing body of council will be able to request the Chair of the committee to address the council and answer any questions about the operation of the committee.

Dismissal of committee members and the Chair

The governing body of council may terminate the engagement of the Chair or a member of the Audit, Risk and Improvement Committee where the Chair or member has:

- breached the conditions of the prequalification scheme
- breached the council's Code of Conduct
- performed unsatisfactorily, or
- declared, or is found to be in, a position of a conflict of interest which is unresolvable.

Termination can only occur with the approval of the Chief Executive of the Office of Local Government and is to be reported to the agency which is responsible for administering the Audit, Risk and Improvement Committee prequalification scheme. Approval is not needed for termination where the Chair or member has become ineligible or removed from the prequalification scheme by the agency administering the scheme. Dismissal is automatic in these situations.

(i) The general manager is to nominate a council employee/s to provide secretariat support to the Audit, Risk and Improvement Committee. Minutes are to be recorded for all committee meetings

The general manager will be required to nominate a council employee/s to provide secretariat support to the Audit, Risk and Improvement Committee. The main functions of this role are to be:

- minuting Audit, Risk and Improvement Committee meetings
- preparing agendas, and
- providing the committee with any information it needs to fulfil its responsibilities.

Core requirement 2:
Establish a risk management framework consistent with current Australian risk management standards

Proposal

It is proposed that:

(a) each council (including county council/joint organisation) is to establish a risk management framework that is consistent with current Australian standards for risk management

(b) the governing body of the council is to ensure that council is sufficiently resourced to implement an appropriate and effective risk management framework

(c) each council's risk management framework is to include the implementation of a risk management policy, risk management plan and risk management process. This includes deciding council's risk criteria and how risk that falls outside tolerance levels will be treated

(d) each council is to fully integrate its risk management framework within all of the council's decision-making, operational and integrated planning and reporting processes

(e) each council is to formally assign responsibilities for risk management to the general manager, senior managers and other council staff and ensure accountability

(f) each council is to ensure its risk management framework is regularly monitored and reviewed

(g) the Audit, Risk and Improvement Committee and the council's internal audit function are to provide independent assurance of risk management activities, and

(h) the general manager is to publish in the council's annual report an attestation certificate indicating whether the council has complied with the risk management requirements.

Description

(a) Each council (including county council/joint organisation) is to establish a risk management framework that is consistent with current Australian standards for risk management

Each council in NSW (including county council/joint organisation) will be required to implement a risk management framework that is consistent with the current Australian risk management standard – currently AS ISO 31000:2018[54]. The framework is to take an enterprise risk management approach which applies to all council activities and risks, not just well-recognised risks such as work health and safety, insurable risks and disaster recovery planning.

[54] Where ISO 31000:2018 is superseded following a future review by the International Organisation of Standardisation or Standards Australia, councils are to conform to the most current Australian risk management standard. AS ISO 31000:2018 can be found at https://www.standards.org.au/standards-catalogue/sa-snz/publicsafety/ob-007/as--iso--31000-colon-2018

The definition of risk management adopted by councils will be the same as that adopted in AS ISO 31000:2018. Risk management comprises of *"coordinated activities to direct and control an organisation with regard to risk"*. Risk is the *"effect of uncertainty on objectives, where an effect is a deviation from the expected. It can be positive, negative or both, and can address, create or result in opportunities and threats"*.

It is recognised that each council will have different risk management requirements depending on its size, needs, budget, complexity of operations and risk management maturity (i.e. the extent to which risk management has already been implemented in the council). Councils will have the flexibility under AS ISO 31000:2018 to choose the size, scope and delivery of their risk management activities so long as they include a number of key structural components (see below).

Where a council wishes to impose requirements that are additional to the proposed framework, it will be able to do so provided the requirements conform to AS ISO 31000:2018 and do not conflict with regulatory requirements.

(b) The governing body of the council is to ensure that council is sufficiently resourced to implement an appropriate and effective risk management framework

The governing body of each council is to provide the resources needed to:

- implement a risk management framework appropriate to the council, and
- deliver the risk treatments and internal controls needed to ensure the council's risks are appropriately managed.

This forms part of the governing body's responsibility for approving the council's budget.

These resources include the necessary:

- human resources (with appropriate skills and experience)
- technology, equipment, tools and information management systems for managing risk
- documented processes and procedures, and
- professional development and training for staff to ensure they can fulfil their risk management responsibilities.

To ensure that the governing body makes informed budgeting decisions, the Audit, Risk and Improvement Committee is to advise the governing body of the resources needed, having regard to any budgetary constraints and the council's operational environment.

Where the Audit, Risk and Improvement Committee considers the resourcing provided for risk management is insufficient relative to the risks facing the council, it is to draw this to the attention of the general manager and the governing body of the council. The Chair of the Committee is to also ensure that the Committee's funding recommendations are minuted by the Committee's secretariat.

The governing body will also be responsible for approving key elements of the council's risk management framework, including the council's risk management policy, risk management plan and risk criteria, following their endorsement by the Audit, Risk and Improvement Committee (see below).

(c) Each council's risk management framework is to include the implementation of a risk management policy, risk management plan and risk management process. This includes deciding the council's risk criteria and how risk that falls outside tolerance levels will be treated

In compliance with AS ISO 31000:2018, each council's risk management framework is to comprise the following key elements:

Risk management policy

Each council will be required to adopt a risk management policy that communicates the commitment of the governing body and the general manager to risk management, and how risk management will be undertaken by the council. The risk management policy is to be approved by the governing body, after endorsement by the Audit, Risk and Improvement Committee.

The council's risk management policy is to describe, at a minimum:

- The council's risk management objectives and priorities, and how these are linked to the council's strategic plans and objectives
- how risk management will be integrated into the overall culture of the council, core business activities and decision-making
- the council's risk criteria
- how the council's risk management policy sits within, and is supported by the council's other policies
- who in the council is accountable and responsible for managing risk in the council
- the resources that will be made available, and
- how the council's risk management performance will be reviewed, measured, reported and improved.

The council's risk management policy can also provide guidance to council staff on the council's commitment to:

- integrating risk management into the council's procedures and practices
- communicating the council's approach to managing risk
- coordinating the interface between risk management and other assurance activities, for example, the Audit, Risk and Improvement Committee, the council's internal audit function and external audit, and
- incorporating risk management into internal staff induction and professional development programs.

The council's risk management policy is to be reviewed at least once each council term, or within one year if there is a significant restructure or change.

Risk management plan

Each council is to develop and implement a risk management plan that provides a structure for how the council will implement its risk management policy and conduct its risk management activities. The chief purpose of the plan is to ensure that the council's arrangements for managing risks are clearly understood and practiced, and identifies where, when and how different types of decisions relating to risk are made across the council and by whom.

To do this, it must include:

- the activities the council will undertake to implement its risk management policy
- roles, accountabilities and responsibilities in relation to risk management
- the timeframes for risk management activities

- how risk management processes will be implemented and maintained (see below)
- resourcing requirements (people, IT and physical assets)
- training and development requirements
- performance measures that will be used to evaluate the success of the council's risk management framework, and
- how and when the council's risk management framework will be reviewed.

Depending on the size, complexity and nature of the council, the council may require a single risk management plan or a hierarchy of linked risk management plans.

The governing body is to approve the council's risk management plan, and any changes made to it, after endorsement by the Audit, Risk and Improvement Committee.

Risk management plans should be living documents and regularly reviewed to reflect current and emerging risks as circumstances change.

Risk management process

The risk management process is a systematic way of identifying, assessing and prioritising risks, deciding how they will be managed, and documenting and communicating this across the council. A summary diagram of the risk management process is provided below.

Each council's risk management process is to include the following stages to ensure its risks are managed effectively. Each stage is to be performed in accordance with AS ISO 31000:2018, using qualitative, semi-quantitative or quantitative methods and techniques that best suit the council's operations, risk management maturity and decision-making needs. NSW Treasury has released a *Risk Management Toolkit for NSW Public Sector Agencies* that councils can use to help them establish their risk management framework[55].

All knowledgeable council staff are to be involved and councils are encouraged to access external expertise where required.

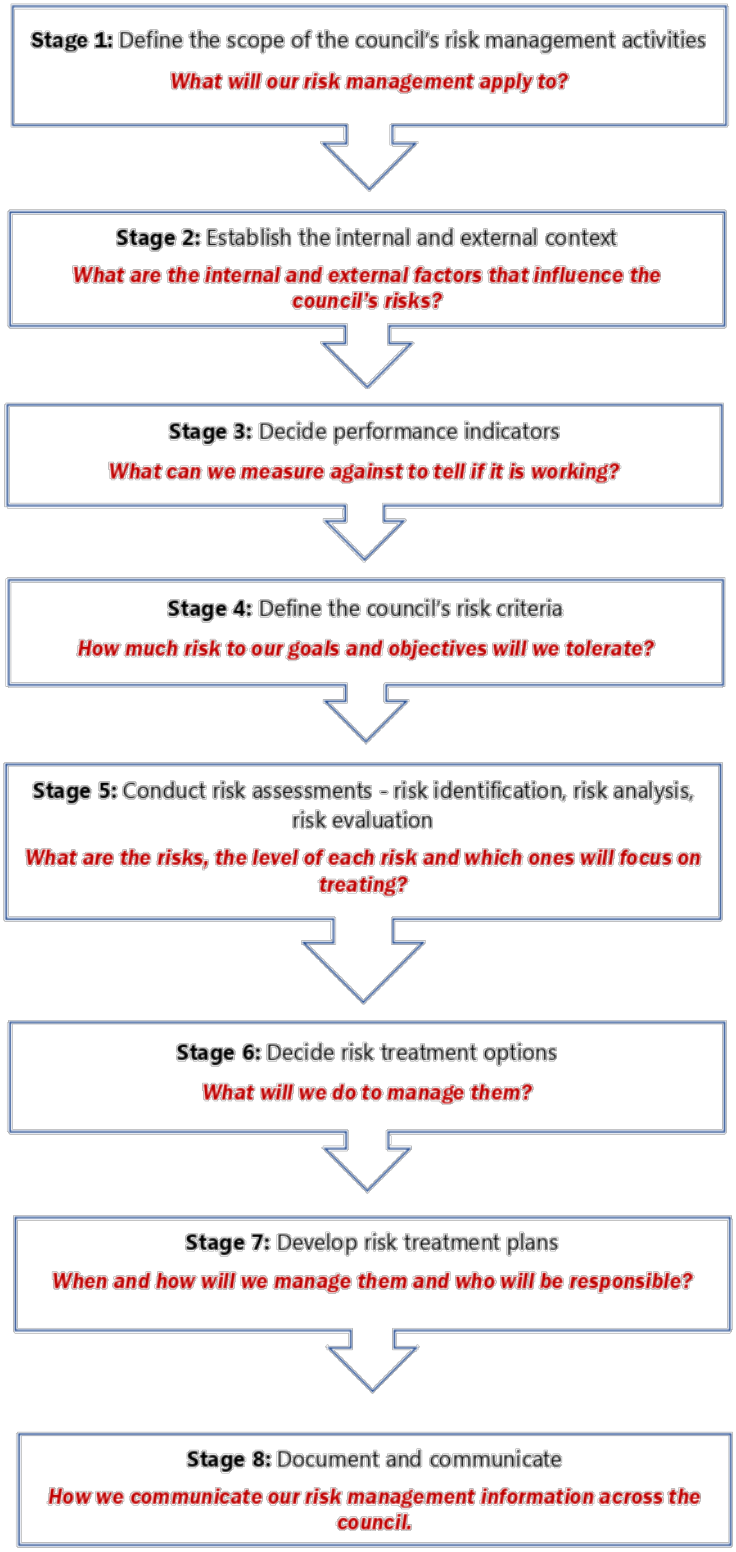
Stage 1: Define the scope of the council's risk management activities

The council is to decide and document the scope of its risk management activities to assist in planning the council's risk management approach. The scope to be decided includes aspects such as:

- the objectives of the council's risk management framework and outcomes expected
- the resources required to plan and develop the framework
- who is responsible for planning and developing the framework
- what records will be kept, and
- what will be the relationship of the risk management framework to other council projects, processes and activities.

[55] The *Risk Management Toolkit for Public Sector Agencies* (TPP 12-03) can be found at https://www.treasury.nsw.gov.au/information-public-entities/governance-risk-and-assurance/internal-audit-and-risk-management/risk

Stages of council's risk management process



Stage 2: Establish the internal and external context

The council is to ensure that it understands and documents the internal and external environment or parameters it operates in and how risk management will impact, and be impacted by these. Factors to be taken into consideration should include internal, political, economic, socio-cultural, technological, legal, and environmental trends and drivers that influence the council's operating environment and can be a source of risk.

Stage 3: Decide performance indicators

The council is to decide the performance indicators it will use to measure the effectiveness of its risk management framework and identify gaps between its actual and desired performance. The performance indicators selected need to be able to be easily measured on an ongoing basis, easily interpreted and understood by staff and management, and provide a meaningful picture of the council's risk management performance.

Stage 4: Define the council's risk criteria

The council is to decide its risk criteria - that is, the amount and type of risk that it is willing to take, or not take, in order to achieve its strategic plan and objectives. It should also define criteria to evaluate the significance of risk based on the council's values, objectives and resources. This will ensure that all council staff have a common understanding of how to evaluate whether a risk is significant and requires a response. It will also ensure that ongoing decision-making about specific activities is consistent across the council.

While the council's risk criteria must be established at the beginning of the risk assessment process, it is dynamic and should be continually reviewed and amended as changes occur to the council's internal or external context.

The council's risk criteria is to be approved by the governing body of the council, after endorsement by the Audit, Risk and Improvement Committee.

Stage 4: Conduct risk assessments

The council is to conduct risk assessments using the following three-step process[56]:

- risk identification – as a first step to assessing what risks need managing, the council is to identify and categorise any risks it is aware of that may help or prevent the council from achieving its strategic goals and objectives. Risk categories could include, for example, council governance risks, fraud and corruption risks, financial risks, compliance risks, risks to council policies, programs and projects, risks to the continuity of operations and services, environmental damage risks, work health and safety risks, purchasing and procurement risks and reporting risks
- risk analysis - once each risk is identified, the council is to assess the effectiveness of any controls that already exist to reduce or enhance the likelihood of a particular event and manage the nature and magnitude of any consequences. This will enable the council to determine the overall level of risk that exists, and
- risk evaluation - once the overall level of risk is determined, the council is to assess and decide which risks require further treatment, and in what order of priority. This is to involve comparing the overall level of risk that exists (based on the risk analysis performed) to the council's risk criteria.

---

[56] In addition to AS ISO 31000:2018, *IEC/ISO 31010 Risk management – risk assessment techniques* provides additional guidance on each step of the risk assessment process. This standard can be found at https://www.iso.org/standard/51073.html

Those risks that fall outside the risk levels the council is willing to tolerate are to be proactively managed. The least tolerable risks are to be given the highest priority.

Stage 5: Decide risk treatment options

The council is to determine a strategy for the treatment of each risk. A decision should be made to either:

- minimise the risk by implementing controls (see stage 6)
- avoid the risk by adopting alternative approaches (for example, revising the timing of a project, choosing a different delivery model)
- transfer the risk to another party which has greater control over the risk, or is less susceptible to the impact of the risk (for example, insurance), or
- accept the risk and develop contingency plans to minimise the impact should the risk eventuate.

Stage 6: Develop risk treatment plans

The council is to develop risk treatment plans that document how the control will be implemented and integrated into the council's day-to-day management and operational processes. Risk treatment plans are to include:

- the rationale, actions to be taken and expected outcome of control
- who is responsible for implementing the control
- resources required
- timeframes, and
- necessary monitoring and reporting, including the performance indicators that will be used to measure the controls effectiveness.

The general manager is to approve the council's risk treatment plans.

Stage 7: Document and communicate

The council is to develop risk reports to summarise and communicate to all staff what risks the council faces. These reports will also be used by the council to regularly review the risk management framework.

Each council's risk reports will vary, dependent on the needs, complexity and risk maturity of each council. At a minimum, however, they should include:

- a risk profile – this is a high-level status report which describes the priorities and management of risk across the council. It provides an overall picture of a council's risk profile, identifies risk priorities, explains the rationale for decisions made about individual risks and allows those responsible for managing particular risks to see how their risks/controls fit into the council's overall risk management framework, and
- risk registers – these describe and prioritise each individual risk, including its cause/s, impact/s and control/s. They also outline who in the council is responsible for managing individual risks.

Risk reports are to be approved by the general manager, following endorsement by the Audit, Risk and Improvement Committee.

(d) Each council is to fully integrate its risk management framework within all of the council's decision-making, operational and integrated planning and reporting processes

The council's risk management framework must be integrated within all of the council's decision-making processes, governance structures, operational procedures and integrated planning and reporting processes for it to be successful.

For effective risk integration to occur, each council must ensure that, in addition to its risk management policy, plan and process, it implements the following supporting elements:

Risk management culture

A poor risk management culture can lead to poor risk management outcomes.

Each council is to foster a positive risk management culture that ensures that the task of managing risks is not seen by management and staff as an additional responsibility or burden, but a normal part of everyday activities and decision-making. A positive risk management culture relies on strong leadership, commitment, reinforcement and communication from the general manager and senior management of the council.

Risk management communication

Poor communication about risk management can lead to a lack of ownership for managing risk.

Each council is to ensure there is clear communication and consultation about risk management to ensure all staff have a common understanding of:

- the basic principles of risk management
- why the council undertakes risk management and how it relates to the council's strategic plans and objectives
- the basis on which decisions within the council are made and the reasons why particular actions are required to manage risk
- the council's risk criteria and risk management policy, plan and priorities
- staff responsibilities and accountabilities for managing certain risks, and
- how to notify new or emerging risks or when something goes wrong or is not working.

The way each council communicates risk management to its staff will vary depending on its needs, organisational structure, existing communication methods and risk maturity. Communication mechanisms could include, for example, specific risk reports relating to key drivers, trends, incidents, risks or business units, formal training programs, information sessions and informal communication such as staff newsletters.

Risk management information system/s

Each council's risk management framework is to be supported by a robust risk management information system that manages risk-related reports, registers, information, documents, policies and procedures. Easy access to information will ensure the council is able to monitor risks/controls and make informed decisions about any further action needed.

The size, complexity and risk management maturity of a council, and the nature of its risk information, will influence the type of risk management information system that it requires. For smaller councils, Microsoft Word or Excel documents that record, report and communicate risk may be appropriate. Larger councils may need to purchase a custom-made product or system.

(e) Each council is to formally assign responsibilities for risk management to the general manager, senior managers and other council staff and ensure accountability

It is the responsibility of all council managers and staff to manage risk.

For risk management to be effective, all staff (permanent, temporary and contractors) must be aware of the risks that relate to their day-to-day roles and activities and their responsibility for managing these risks and following risk management policies and procedures.

To provide accountability, risk management responsibilities are to be clearly articulated in the job descriptions and performance measurement processes of all relevant managers and staff.

Managers and staff with risk management responsibilities are to also have the necessary skills, knowledge and experience required to fulfil their risk management responsibilities, as well as attitudes and behaviours that support risk management.

General manager and senior managers

Consistent with the general manager's role under section 335 of the Local Government Act to conduct the day-to-day management of the council, the general manager will have ultimate responsibility and accountability for risk management in the council.

This includes:

- approving the council's risk management plan, risk treatment plans, risk register and risk profile
- recommending the council's risk management policy and risk criteria for the endorsement of the Audit, Risk and Improvement Committee and approval of the governing body
- overseeing the council's risk management framework and ensuring it is effectively communicated, implemented and reviewed regularly
- promoting and championing a positive risk culture
- ensuring that all council managers and staff (permanent, temporary or contract) understand their risk management responsibilities and that these are included in all job descriptions, staff induction programs, performance agreements and performance appraisals
- annually attesting that council's risk management framework complies with statutory requirements, and
- approving the council's implementation of corrective actions recommended by the council's internal audit function, external audit and Audit, Risk and Improvement Committee.

Depending on the council's needs, resources and organisational structure, and to assist the integration of risk management across the council, the general manager may wish to delegate key aspects of the council's risk management framework to a group of senior managers established for this purpose. The senior management group would report to the general manager on risk management issues.

Tasks delegated to a council's senior management group could include:

- developing the council's risk management policy
- determining the council's risk criteria
- leading the risk management process - for example, evaluating the council's internal and external context, identifying, assessing and prioritising risks and developing risk treatment plans and internal controls
- developing the council's risk register and risk profile
- communicating and implementing the council's risk management policy and plans across council

- advising/reporting on the performance and implementation of the council's risk management framework to the general manager, and
- reviewing recommendations for corrective actions from the Chief Audit Executive and council's internal audit function and determining council's response.

The senior management group is to meet regularly to enable it to fulfil its functions. Council's Risk Management Coordinator is to attend senior management group meetings. The senior management group can also invite the Chief Audit Executive.

Responsibilities for risk management assigned to the general manager and senior managers are to be included in their employment contract and performance reviews.

Risk Management Coordinator and risk management function

The general manager is to appoint a Risk Management Coordinator who will be responsible for the day-to-day activities required to implement the council's risk management framework and provide specialist risk management skills and knowledge.

The Risk Management Coordinator is to report directly to the general manager or a member of the senior management group in relation to council's risk management function.

Whilst this role has been titled as the 'Risk Management Coordinator', councils will be free to use whatever title they wish to refer to this function (for example, Chief Risk Officer, Risk Manager etc.).

The role and responsibilities of the Risk Management Coordinator are to include:

- supporting the senior management group by coordinating and providing clear and concise risk information, advice and/or reports that can be used in planning and decision-making
- coordinating the various activities relating to risk management within the council
- helping to build a risk management culture within the council, including facilitating and driving risk management at the strategic and operational level within the council and ensuring consistency in practice
- ensuring there are easily accessible systems and processes in place to enable all staff to conveniently undertake risk management in their day-to-day work
- ensuring risk management processes are applied consistently across the council
- organising appropriate staff risk management training and development
- developing and maintaining a risk reporting framework to enable regular advising/reporting of key risks, and the management of those risks, to the senior management group
- supporting council staff with their risk management obligations and providing staff with advice and tools to ensure risk management compliance
- implementing effective risk management communication mechanisms and information system/s
- establishing and maintaining an ongoing monitoring system to track the risk management activities undertaken within council and assessing the need for further action
- assessing risk management information for completeness, accuracy and consistency (for example, risk registers, risk treatment plans), and
- preparing advice or reports for the Audit, Risk and Improvement Committee and attending Committee meetings (where requested).

In order to fulfil their role, the Risk Management Coordinator must:

- have a well-developed understanding of the council and its operations
- have the skills, knowledge and leadership qualities required to support and drive risk management
- have sufficient authority to intervene in instances where risk management efforts are being hampered by a lack of cooperation or through lack of risk management capability or maturity, and

- be able to add value to the risk management process by providing guidance and support in managing difficult risk, or risks spread across a number of the council's business units or operational areas.

Each council will have the flexibility to establish its risk management function based on its structure, resourcing, risk management needs and risk management maturity.

For some councils with larger budgets and higher risks, the Risk Management Coordinator will require dedicated staff to help implement the council's risk management framework. For other councils, their size and risk profile may not justify additional risk management staff and the Risk Management Coordinator will be sufficient.

While best practice would see a stand-alone Risk Management Coordinator employed by each council, it is recognised that some smaller or rural councils may find it difficult to employ a stand-alone Risk Management Coordinator due to the cost involved, the council's remote location and/or that the council's risk management framework may not require a full-time stand-alone employee.

Councils will, therefore, be able to combine the Risk Management Coordinator's role with other council responsibilities (including the Chief Audit Executive) provided that there are adequate safeguards put in place by the council to limit any cognitive bias (which can lead to faulty risk assessments and decision-making errors).

Depending on the specific needs and circumstances of the council, these safeguards could include:

- the Audit, Risk and Improvement Committee being informed of the Risk Management Coordinator's additional role, including the reporting lines, responsibilities and expectations related to the role
- any potential issues or conflicts of interest arising from the other operational roles held by the Risk Management Coordinator being formally documented and communicated to the Audit, Risk and Improvement Committee
- the Risk Management Coordinator being prohibited from undertaking risk management evaluations and reviews in relation to the council operations they are responsible for. Another senior staff member will conduct these and will report directly to the general manager on the results
- if the Chief Audit Executive and Risk Management Coordinator is a combined role, any independent review of council's risk management framework must be undertaken by an independent external party, and
- the Audit, Risk and Improvement Committee regularly assessing that the safeguards put in place are effective.

Council managers

Responsibility for managing specific policy, project and program risks generally rests with council managers across the council. This includes council managers being responsible, within the sphere of their authority, for:

- promoting awareness of risks and risk treatments that must be implemented
- ensuring council staff are implementing the council's risk management framework as developed and intended and performing their risk management responsibilities
- identifying risks that will affect the achievement of the council objectives
- establishing and/or implementing specific policies, operating and performance standards, budgets, plans, systems and/or procedures to manage risks, and
- monitoring the effectiveness of risk treatment and internal controls.

All other council staff

All council staff are to be responsible for:

- helping to identify risks in their business unit
- implementing risk treatment plans within their area of responsibility
- following standard operating procedures (where applicable), and
- communicating or escalating new risks that emerge to their manager.

(f) Each council is to ensure its risk management framework is regularly monitored and reviewed

The senior management group is to establish and maintain an ongoing monitoring and review process of the information gathered from council's risk management process[57] to ensure its risk management framework is up-to-date and relevant. It will also enable the senior management group to report to the general manager, governing body of the council and Audit, Risk and Improvement Committee when required about the council's risk management framework.

Each council is to base its ongoing monitoring and review process based on its own needs, however, this should include at a minimum the following two key elements:

1. **Quarterly advice from the Risk Management Coordinator to the senior management group assessing the council's risk profile and risk registers** – this will ensure that risks are being correctly identified, prioritised and treated, and any emerging problems are known and rectified quickly. Any changes are to be captured in updates to the council's risk profile and risk register, and relevant risk treatment plans.

2. **An annual self-assessment at the end of each financial year by the senior management group of the quality of the council's risk management framework** – this is to assess the operation of the risk management framework during the preceding financial year and to ensure:
    - the council is providing sufficient resources for risk management and staff are able to carry out their risk management responsibilities
    - the council's risk management framework complies with AS ISO 31000:2018
    - the council's risk management framework operates effectively and supports the achievement of council's strategic goals and objectives
    - management has embedded a positive risk culture
    - the council's risk criteria is appropriately reflected in council's internal control framework
    - the council takes an enterprise risk management approach that is fully integrated into all aspects of the council, including decision-making processes and operations
    - risks are formally considered when developing and implementing all council policies, programs, projects and other activities, including procurement
    - risk management covers all relevant risk categories including strategic, operational, compliance, reputational and reporting risks
    - major risks have been identified and assessed by the council and appropriate risk treatments have been implemented that reflect the council's risk criteria
    - the council's internal controls are effective and appropriate
    - the council's risk register and risk profile is current and appropriate

[57] This includes ongoing monitoring and review of the scope of the council's risk management framework, the context the council operates in, the council's risk criteria, the results of the council's risk assessment, controls implemented, risk treatment plans and risk reports such as the council's risk profile and risk registers

- risk information is captured and communicated in a timely manner across the council, enabling management and staff to carry out their responsibilities, and
- the council's risk management policies, procedures and plans are being complied with.

Ultimately the general manager is responsible for the implementation of the council's risk management framework, and ensuring that risks are being managed appropriately. Each council will have the flexibility to decide, based on its own needs and resources, how and when the senior management group reports risk information to the general manager and the governing body of the council.

Standards Australia has released *HSB 158-2010 Delivering assurance based on ISO 31000:2009 Risk management – Principles and guidelines*[58] which may assist councils to monitor and review their risk management frameworks.

Performance management system

The senior management group is to ensure the effectiveness of the risk management framework can be assessed. This will require the senior management group and Risk Management Coordinator to ensure that:

- approved risk treatment plans have performance targets that can be measured against goals and objectives, and
- a data collection system is maintained to obtain the data needed to measure the impact of the council's risk management framework.

Performance targets are to be set annually by the senior management group, in consultation with the general manager and the Audit, Risk and Improvement Committee.

(g) The Audit, Risk and Improvement Committee and the council's internal audit function are to provide independent assurance of risk management activities

Role of the Audit, Risk and Improvement Committee

The Audit, Risk and Improvement Committee will be responsible for providing independent assurance to the general manager and governing body that the council's risk management framework is appropriate and working effectively.

This includes advising whether:

- the council is providing sufficient resources for risk management and staff are able to carry out their risk management responsibilities
- the council's risk management framework complies with AS ISO 31000:2018
- the council's risk management framework operates effectively and supports the achievement of the council's strategic goals and objectives
- management has embedded a positive risk management culture
- the council's risk criteria is appropriately reflected in the council's internal control framework
- the council takes an enterprise risk management approach that is fully integrated into all aspects of the council, including decision-making processes and operations

[58] More information about HSB 158-2010 can be found at https://www.standards.org.au/standards-catalogue/sa-snz/publicsafety/ob-007/hb--158-2010. Please note that this standard is based on the previous risk management standard ISO 3100:2009 and may possibly be updated.

- risks are formally considered when developing and implementing all council policies, programs, projects and other activities, including procurement
- risk management covers all relevant risk categories including strategic, operational, compliance, reputational and reporting risks
- major risks have been identified and assessed by the council and appropriate risk treatments have been implemented that reflect the council's risk criteria
- the council's internal controls are effective and appropriate
- the council's risk register and risk profile is appropriate
- risk information is captured and communicated in a timely manner across the council, enabling management and staff to carry out their responsibilities
- there are council-specific, fit-for-purpose tools, systems and processes to help all those responsible for managing risk to fulfil their responsibilities, and
- the council's risk management policies, procedures and plans are being complied with.

The Audit, Risk and Improvement Committee's role and responsibilities in relation to risk management are to be documented in its terms of reference.

The frequency and nature of the Committee's assurance to the general manager and governing body is to be determined by the Committee in consultation with the general manager and governing body of the council.

At a minimum, the Audit, Risk and Improvement Committee is to be required to provide an annual assessment of the council's risk management framework as part of its annual assurance report to the governing body of the council. This will ensure that the governing body of the council receives the Committee's independent and objective opinion about the risk management activities conducted each year. It will also support the governing body in the exercise of its oversight role under the Local Government Act.

Reporting to the Audit, Risk and Improvement Committee

The Audit, Risk and Improvement Committee is to determine in consultation with the general manager what information it needs from the council to fulfil its risk management assurance role. Information requirements are to be based on the council's risk management maturity, the resources available and the aspect of the risk management framework being assessed.

Review or information requirements could include, for example:

- advice from the senior management group to each quarterly meeting of the Audit, Risk and Improvement Committee providing an overview of the council's risks and controls and whether significant risks have been identified, assessed and responded to appropriately
- annual advice from the senior management group about the implementation of the council's risk management framework - for example, whether it conforms with AS ISO 31000:2018, the risk process has been implemented effectively, there is a positive risk culture, the council's risk register and profile are appropriate, the council's risk management policy and procedures are being complied with, and/or
- an independent strategic review by the internal audit function or an external party at least once each council term (i.e. four years) assessing adequacy of the risk management framework.

The Audit, Risk and Improvement Committee will also be informed by any findings or recommendations made by the council's external auditor in relation to risk management.

The senior management group will be required to develop an action plan for the general manager and the Audit, Risk and Improvement Committee to address any risk management issues identified by the Committee.

Role of the internal audit function

The council's internal audit function will support the Audit, Risk and Improvement Committee to fulfil its assurance responsibilities through the audit of particular risks, as identified in the internal audit function's work plan. The role of the council's internal audit function in relation to risk management is to be documented in the council's Internal Audit Charter.

Given the need to maintain the independence and objectivity of the internal audit function, the following boundaries are to apply with respect to the role of the internal audit function in the council's risk management framework:

- it is to be clear that council management remains responsible for risk management
- the internal audit function is to provide advice, challenge and support management's decision-making, as opposed to taking risk management decisions themselves
- the internal audit function should not:
  - manage any of the risks on behalf of the council
  - set the council's risk criteria
  - impose risk management processes
  - decide or implement risk responses, or
  - be held accountable for risk management activities.

(h) The general manager is to publish in the council's annual report an attestation certificate indicating whether the council has complied with the risk management requirements

The general manager will be required to annually publish an attestation statement in the council's annual report indicating whether, during the prior financial year, the council was 'compliant', 'non-compliant' or 'in transition' against each of the above-mentioned requirements of the council's risk management framework.

Compliance status is to be self-assessed based on the results of the senior management group's annual self-assessment. The table on page 84 lists the proposed compliance categories and follow-up action that will be required.

The general manager is to ensure that a copy of the attestation statement and the exception approval from the Chief Executive Officer of the Office of Local Government (if applicable) is published in the council's annual report. A copy of the attestation statement is to also be provided to the Office of Local Government.

The Chair of the Audit, Risk and Improvement Committee is to also sign the attestation statement where he/she agrees that it is a true and accurate reflection of the council's compliance status against statutory requirements.

Core requirement 3:
Establish an internal audit function mandated by an Internal Audit Charter

Proposal

It is proposed that:

(a) each council (including county council/joint organisation) is to establish an internal audit function

(b) the governing body is to ensure that the council's internal audit function is sufficiently resourced to carry out its work

(c) the governing body of the council is to assign administrative responsibility for internal audit to the general manager and include this in their employment contract and performance reviews, and

(d) the Chief Audit Executive is to develop an Internal Audit Charter, based on a model charter, which will guide how internal audit is conducted by the council. This Charter is to be approved by the governing body of council after endorsement by the Audit, Risk and Improvement Committee.

Description

(a) Each council is to establish an internal audit function

Each council in NSW, (including county council/joint organisation), will be required to have an internal audit function that reports functionally to the Audit, Risk and Improvement Committee and is independent from council management.

The definition of internal audit adopted by councils will be the same as that adopted in the IPPF - internal audit is *"an independent, objective, assurance and consulting activity designed to add value and improve [council's] operations. It helps [council] accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control and governance processes".*

It is recognised that each council will have different internal audit requirements depending on its size, needs, budget and complexity of operations. To provide councils greater flexibility, each council will have the freedom to determine the size and scope of their internal audit activities. Councils will also have the flexibility to decide how to deliver their internal audit function. They can either:

- establish a stand-alone internal audit function for their exclusive use
- utilise a joint internal audit function established by their joint or regional organisation of councils that is shared by member councils, or
- share their internal audit function with another council/s in close proximity or of their choosing as part of an independent shared arrangement.

It is recommended that county councils, due to their size, enter into a share arrangement with one of their member councils or utilise an internal audit function established by a joint or regional organisation of councils.

Some of the requirements for shared arrangements will differ from those of stand-alone internal audit functions established for a council's exclusive use (as described in core requirements 1-8). Core requirement 9 outlines the specific requirements of shared arrangements.

Where a council wishes to impose requirements that are additional to the proposed framework, it will be able to do so provided the requirements comply with the IPPF and do not conflict with statutory requirements.

(b) The governing body is to ensure that council's internal audit function is sufficiently resourced to carry out its work

The governing body will be required to ensure that the council's internal audit function is sufficiently resourced to effectively carry out its work[59]. This is in line with the governing body's responsibility for the council's budget and other resourcing decisions. To ensure that the governing body makes informed budgeting decisions, the Audit, Risk and Improvement Committee is to advise the governing body of the resources needed.

Where the Audit, Risk and Improvement Committee considers the resourcing provided for internal audit activities is insufficient relative to the risks facing the council, it is to draw this to the attention of the general manager and the governing body of the council. The Chair of the Committee is to also ensure that the Committee's funding recommendations are minuted by the Committee's secretariat.

(c) The governing body of the council is to assign administrative responsibility for internal audit to the general manager and include this in their employment contract and performance reviews

Consistent with the general manager's role under section 335 of the Local Government Act to conduct the day-to-day management of the council, the general manager will be responsible for the **administrative** delivery of council's internal audit function. This means that the general manager will be required to:

- advise the governing body of the funding needed to adequately resource the internal audit function when making final budget decisions
- align the internal audit budget to approved work plans and recommendations made by the Audit, Risk and Improvement Committee
- allocate the funds needed to engage internal audit personnel or external providers with the technology, skills and experience necessary to meet the risk and assurance needs of the council
- provide appropriate administrative support, for example, access to council's human resources networks, payroll, work health and safety, office facilities and resources etc., and
- ensure that the councils internal audit activities are appropriately positioned within the council to work with external audit and internal business units and to operate independently.

The general manager will have no role in the exercise of the internal audit (for example, the conduct of internal audits, development of work plans, audit techniques used, reporting to the governing body and Audit, Risk and Improvement Committee etc.). The general manager's administrative responsibilities in relation to internal audit are to be included in the general manager's employment contract and regular performance reviews to ensure accountability. The Office of Local Government will amend the general manager's standard contract under section 338 of the Local Government Act to reflect this requirement.

---

[59] The Institute of Internal Auditors has developed the *Audit Intelligence Suite* which can be used to obtain a general picture of the potential resources needed for an internal audit function based on benchmark costs across the corporate and public sectors. For access (cost involved), go to https://www.theiia.org/centers/aec/Pages/benchmarking.aspx

(d) The Chief Audit Executive is to develop an Internal Audit Charter, based on a model charter, which will guide how internal audit is conducted by the council. This Charter is to be approved by the governing body of the council after endorsement by the Audit, Risk and Improvement Committee

Each council will be required to adopt an 'Internal Audit Charter' to guide how internal audit will be undertaken by that council and measure its effectiveness.

The Internal Audit Charter is to be developed by the council's Chief Audit Executive in consultation with the Audit, Risk and Improvement Committee and approved by the governing body of the council after endorsement by the Committee.

Each council's Internal Audit Charter is to comply, at a minimum, with a Model Internal Audit Charter[60]. This is consistent with councils being required to adopt policies based on other model documents (for example, the Model Code of Conduct and the Model Code of Meeting Practice).

The Model Internal Audit Charter will:

- define the purpose, authority and responsibility of the internal audit function
- establish internal audit's position, role and responsibilities within the council
- describe the importance of the independence of the internal audit function and how this will be maintained
- define the roles and responsibilities of those involved in the council's internal audit activities
- assign responsibility for appointing and dismissing the Chief Audit Executive
- describe how internal audit activities are to be undertaken (i.e. the scope of assessments, writing internal audits and work plans, performing internal audits, communicating results, writing audit reports and monitoring the implementation of corrective actions)
- describe the quality assurance and improvement program
- describe administrative arrangements, HR support and budget provided to support the internal audit function
- define reporting relationships
- define internal audit's relationship with the external auditor, and
- authorise access to internal audit information.

Councils will be able to include additional provisions in their Internal Audit Charter so long as they do not conflict with the Model Internal Audit Charter or the IPPF. This will ensure any matters not contemplated by the Model Charter are addressed by councils in a robust way that complies with internationally recognised standards.

Where the council's Internal Audit Charter contains additional provisions not included in the Model Internal Audit Charter, the Chief Audit Executive is to review the Charter annually as part of the council's internal audit quality assurance and improvement program. A strategic review is to also be undertaken once each council term (i.e. four years).
Changes to the Charter are to be approved by the governing body of the council after endorsement by the Audit, Risk and Improvement Committee.

---

[60] The Model Internal Audit Charter will be drafted by the Office of Local Government in consultation with councils based on the final internal audit framework developed following consultation on this discussion paper

Core requirement 4:
Appoint internal audit personnel and establish reporting lines

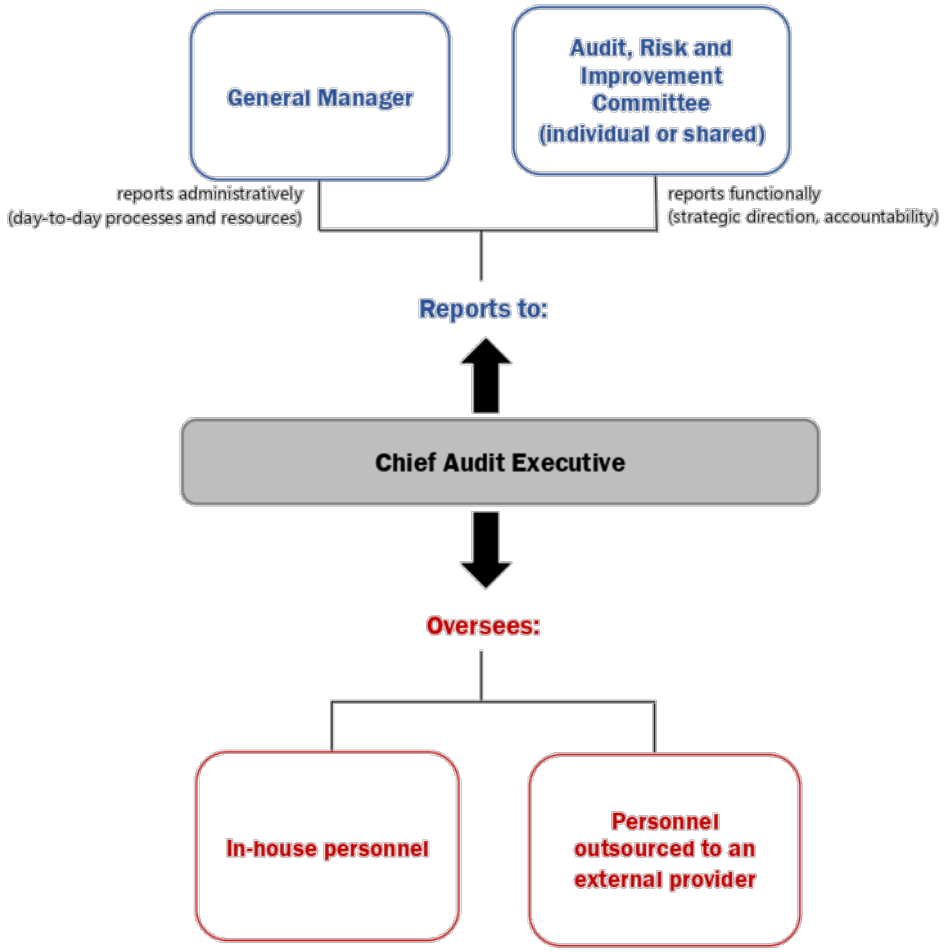
Proposal

It is proposed that the:

(a) general manager is to appoint a Chief Audit Executive to oversee the council's internal audit activities in consultation with the Audit, Risk and Improvement Committee

(b) Chief Audit Executive is to report functionally to the Audit, Risk and Improvement Committee and administratively to the general manager and attend all committee meetings, and

(c) general manager is to ensure that, if required, the council has adequate internal audit personnel to support the Chief Audit Executive. Councils will be able to appoint in-house internal audit personnel, or completely or partially outsource their internal audit function to an external provider.



Description

(a) The general manager is to appoint a Chief Audit Executive to oversee the council's internal audit activities in consultation with the Audit, Risk and Improvement Committee

Attributes of the Chief Audit Executive

The general manager, in consultation with the Chair of the Audit, Risk and Improvement Committee, will be required to appoint a Chief Audit Executive to oversee the council's internal audit activities. The term 'Chief Audit Executive' has been used throughout this discussion paper to reflect the terminology used in the IPPF and NSW public sector internal audit model. However, each council is able to describe this role as it chooses, for example, Chief Internal Auditor, Chief Audit Officer etc.

The Chief Audit Executive is to

- be independent, impartial, unbiased and objective when performing their work and free from conflicts of interest. This also means that the Chief Audit Executive cannot undertake internal audit activities on any council operations or services that he/she has held responsibility for within the last five years
- be a council employee and the most senior member of staff in council responsible for internal audit (but not the general manager or council's senior financial officer)
- cannot be outsourced to an external service provider, except where the council has entered into a shared arrangement with another council or as part of their joint or regional organisation of councils
- possess the following skills, knowledge and experience to effectively carry out their role:

  Essential
  - the credibility to ensure they are able to negotiate on a reasonably equal footing with the general manager and councillors of the council, as well as the Audit, Risk and Improvement Committee, and
  - the skills, knowledge and personal qualities necessary to lead credible and accepted internal audit activities in the council

  Preferred
  - high-level experience overseeing internal audit, and
  - appropriate professional certifications such as those recognised by the Institute of Internal Auditors (Certified Internal Auditor), Certified Professional Accountants Australia or Chartered Accountants Australia and New Zealand.

This will ensure that the internal audit function of each council is led by someone with the skills, knowledge, experience and integrity needed to establish and effectively oversee a council's internal audit functions. It will also ensure that the council retains control of the internal audit strategic direction and is able to monitor the performance of any external service provider.

Oversight

It is important that the Chief Audit Executive has the functional independence to ensure that this role has the freedom necessary to independently assess and report on the way council operates. However, the Chief Audit Executive, as a member of staff under the Local Government Act, must also be appointed by and accountable to the general manager.

As a safeguard, to ensure the functional independence of the Chief Audit Executive, the general manager is to consult with the Chair of the Audit, Risk and Improvement Committee before appointing or dismissing the Chief Audit Executive, or making any change to the Chief Audit Executive's

employment conditions. Where dismissal occurs, the general manager is to report to the governing body advising of the reasons why the Chief Audit Executive was dismissed.

Where the Chair of the Audit, Risk and Improvement Committee has any concerns about the treatment of the Chief Audit Executive, or any action taken that may compromise the Chief Audit Executive's ability to undertake their functions, they must report their concerns to the governing body of the council.

Responsibilities

The key responsibilities of the Chief Audit Executive include:

- managing the day-to-day direction and performance of the council's internal audit activities to ensure they add value to council
- supporting the operation of the Audit, Risk and Improvement Committee
- ensuring the council's internal audit activities comply with statutory requirements, the IPPF and the council's needs
- developing, implementing and reviewing the council's Internal Audit Charter, policies and procedures, work plans and quality assurance and improvement program
- providing advice to the Audit, Risk and Improvement Committee and governing body of the council on the adequacy and effectiveness of the council's governance frameworks, risk management practices and internal controls
- confirming the implementation by the council of corrective actions that arise from the findings of internal audit activities, and
- managing internal audit personnel and ensuring that they have the skills necessary to perform audits and are up to date on current issues affecting the council and on audit techniques and developments.

Where a council has outsourced its internal audit activities to an external provider, the Chief Audit Executive will be responsible for:

- overseeing the service contract and the quality of audits conducted by the external provider (including overseeing the quality assurance and improvement program)
- ensuring that the council retains control of the strategic direction of internal audit activities
- reporting to the general manager and the governing body of the council on the adequacy and effectiveness of the council's governance frameworks, risk management practices and internal controls (based on the findings provided by the external provider)
- confirming the council's implementation of corrective actions that arise from the findings of audits
- developing policies and procedures that guide the audits conducted by the external provider
- developing the internal audit annual work plan and strategic plan
- ensuring audit methodologies used by the external provider comply with the IPPF and are accessible to the council (subject to any licensing restrictions), and
- supporting the operation of the Audit, Risk and Improvement Committee.

Combining Chief Audit Executive with other responsibilities

It is recognised that some smaller rural councils may find it difficult to employ both a stand-alone Chief Audit Officer and stand-alone Risk Management Coordinator due to the cost involved, council's remote location and/or that the council's risk management function and internal audit function may not require full-time stand-alone employees.

Whilst it is not best practice, it is recognised that combining the Chief Audit Officer role with the Risk Management Coordinator role may make it easier for smaller or remote councils to establish their risk management framework and internal audit function.

Councils will, therefore, be able to combine the Chief Audit Officer's role with the Risk Management Coordinator role provided there are adequate safeguards put in place by the council to limit any real or perceived bias or conflicts of interest that may lead to faulty decision-making and cognitive bias. The endorsement of the Audit, Risk and Improvement Committee will also be required before the combined role can commence.

Depending on the specific needs and circumstances of the council, safeguards could include:

- the Audit, Risk and Improvement Committee being informed of the Chief Audit Executive's dual role, including reporting lines, responsibilities and expectations related to the role
- any potential issues or conflicts of interest arising from the dual role being formally documented in council's Internal Audit Charter
- internal audit briefs being reviewed by the Audit, Risk and Improvement Committee to ensure adequate coverage of the proposed audit, where it concerns any key risks overseen by the Chief Audit Executive in their role as Risk Management Coordinator
- the Audit, Risk and Improvement Committee, or a qualified external party, reviewing internal audit findings and recommendations before they are finalised
- the council's quality assurance program including an external assessment of the Chief Audit Officer's independence and objectivity (for internal audit purposes) in relation to their Risk Management Coordinator role, and
- the Audit, Risk and Improvement Committee regularly assessing that the safeguards put in place are effective.

(b) The Chief Audit Executive is to report functionally to the Audit, Risk and Improvement Committee and administratively to the general manager, and attend all committee meetings

To ensure that internal audit operates independently, the Chief Audit Executive will have a dual reporting line and report:

- **administratively to the general manager** - to facilitate the day-to-day operations of internal audit (for example, in relation to budgeting, accounting, internal audit staff leave and disciplinary matters, internal communications, administration of policies and procedures), and
- **functionally to the Audit, Risk and Improvement Committee** - for the strategic direction, performance and accountability of internal audit activities and personnel.

The general manager must not take any action impacting on the employment of the Chief Audit Executive, including through performance management or disciplinary processes, without consulting with the Chair of the Audit, Risk and Improvement Committee.

The Chief Audit Executive will be required to confirm at least annually to the Audit, Risk and Improvement Committee the independence of internal audit activities.

Access to council staff and information

To achieve the degree of independence necessary to effectively carry out internal audit activities, the Chief Audit Executive will automatically have direct and unrestricted access to the general manager and senior managers of the council, as well as the Audit Risk and Improvement Committee (through the Chair).

Any council staff member or contractor will also be able to directly alert the Chief Audit Executive of emerging risks or internal audit related issues.

The Chief Audit Executive is to have direct and unrestricted access to all council staff, resources and information necessary for the performance of internal audit activities.

Reporting concerns about councillors or council staff

Where a Chief Audit Executive has concerns regarding the general manager or senior council staff, they will be able to:

- raise their concerns with the Chair of the Audit, Risk and Improvement Committee (if it relates to the effectiveness of the internal audit function)
- report breaches of the council's Code of Conduct to the general manager, or by the general manager to the Mayor[61]
- report their concerns through the council's internal reporting policy, complaints handling policy or other associated protocols, and/or
- make a public interest disclosure under the *Public Interest Disclosures Act 1994* to the:
  - Independent Commission Against Corruption (concerning corrupt conduct)[62]
  - NSW Ombudsman (concerning maladministration)
  - NSW Auditor General (concerning serious and substantial waste of public money)
  - Office of Local Government (concerning serious and substantial waste in local government and breaches of pecuniary interest obligations), and/or
  - Information and Privacy Commissioner (concerning government information contraventions).

Code of Conduct

The Chief Audit Executive is to comply with the council's Code of Conduct, as well as the Code of Ethics in the IPPF.

Breaches of the council's Code of Conduct by the Chief Audit Executive are to be reported in writing to the general manager of the council in the first instance. The general manager should notify the Chair of the Audit, Risk and Improvement Committee of any such allegations and their outcome.

(c) The general manager is to ensure that, if required, the council has adequate internal audit personnel to support the Chief Audit Executive. Councils will be able to appoint in-house internal audit personnel or to completely or partially outsource their internal audit function to an external provider

Regardless of size, each council will be required to have an appropriately resourced internal audit function when section 428A of the Local Government Act commences.

For some councils with larger budgets and higher risks, this will require dedicated internal audit staff to support the Chief Audit Executive to deliver the internal audit function. For other councils, their size and risk profile may not justify additional internal audit staff and the Chief Audit Executive will be sufficient.

For councils that require additional internal audit personnel, options include having a dedicated in-house team, co-sourcing arrangements, or outsourcing their audits to an external provider.

---

[61] As required by the *Procedures for the Administration of the Model Code of Conduct for Local Councils in NSW*

[62] Under section 11 of the *Independent Commission Against Corruption Act 1988*, the Chief Audit Executive must report any suspected corrupt activity to the Independent Commission Against Corruption

In determining the most appropriate option for the delivering the council's internal audit function, the general manager should consider the:

- size of the council in terms of both staffing levels and budget
- geographical and functional distribution of the council's operations
- complexity of the council's core business
- risk profile of the council's operations
- council's integrated planning and reporting framework
- the viability of alternative service delivery models (for example, whether council could attract and retain suitable in-house internal audit staff or experienced contract managers for out-sourced service delivery)
- overall cost of alternative service delivery models, including the salaries and overheads of in-house internal audit personnel compared to the costs of contract management and delivery for out-sourced services, and
- capacity of alternative service delivery models to deliver flexibility in the internal audit work plan.

Whichever model a council chooses, the internal audit function, including the appointment of internal audit personnel, is to be overseen by the Chief Audit Executive.

The Chief Audit Executive must be a council employee and cannot be outsourced, other than through a shared arrangement with another council or through a joint or regional organisation of councils.

Employing in-house internal audit personnel

Internal audit personnel report directly to the Chief Audit Executive.

In-house internal audit personnel can be appointed on a full-time or part-time basis. They will be required to comply with the council's Code of Conduct and the Code of Ethics in the IPPF and are to have no executive, managerial or operational powers, authorities, functions or duties except those relating to internal audit. They also cannot have any responsibility for managing any risks or implementing any audit recommendations, including those made by external audit.

Position descriptions for in-house internal audit staff are to require:

- appropriate qualifications
- proficiency in internal audit and accounting principles and techniques (particularly if working extensively with financial information and reports)
- knowledge of economics, management practices, commercial law, taxation, finance, quantitative methods, fraud and internal audit technology, and
- effective interpersonal and communication skills.

Outsourcing internal audits to an external provider

Providing that independence requirements are adhered to, councils can contract their internal audit function to an external internal audit service provider. Examples of providers include private sector accounting firms with a specialist internal audit division, boutique firms that specialise in internal audit, and internal audit contractors.

The advantages of using external providers for internal audit activities include[63]:

- flexibility
- access to a wide range of expertise
- the ability to access the service as and when required, and
- the ability to pool resources with other councils to purchase external services as part of a shared arrangement.

Disadvantages include loss of corporate knowledge, lack of proximity and possible increased costs.

If a council chooses to outsource its internal audits, the Chief Audit Executive is to be the contract manager of the service and is to ensure that:

- an appropriately qualified external provider is conducting the audit in compliance with relevant standards
- the performance of the external provider is actively monitored, and
- the external provider:
  - does not undertake audit work regarding operations or services they have been responsible for, or consulted on, within the last two years
  - is not the same auditor providing council's external audit services
  - is not the auditor of any contractors of the council (and therefore subject to council's internal audits)
  - does not undertake other contract work for the council in addition to internal audit
  - has authority to implement the work program approved by the Audit, Risk and Improvement Committee
  - is rotated, or some other method is established, to address risks caused from having the same auditors auditing the same unit/functional area over a prolonged period of time, and
  - uses audit methodologies that comply with the IPPF and are accessible to the council (subject to any licensing restrictions that may be in place).

[63] *Internal Audit in Australia* published by The Institute of Internal Auditors - Australia (2016) provides a useful comparison of the advantages and disadvantages of different internal audit function delivery models (page 23 onwards).

Core requirement 5:
Develop an agreed internal audit work program

Proposal

It is proposed that, for each council, the Chief Audit Executive will:

(a) develop a four-year strategic plan to guide the council's longer-term internal audits in consultation with the governing body, general manager and senior managers. The strategic plan is to be approved by the Audit, Risk and Improvement Committee

(b) develop an annual risk-based internal audit work plan, based on the strategic plan, to guide the council's internal audits each year. The work plan is to be developed in consultation with the governing body, general manager and senior managers and approved by the Audit, Risk and Improvement Committee, and

(c) ensure performance against the annual and strategic plans can be assessed.

Description

(a) The Chief Audit Executive is to develop a four-year strategic plan to guide the council's longer-term audits in consultation with the governing body, general manager and senior managers. The strategic plan is to be approved by the Audit, Risk and Improvement Committee

The Chief Audit Executive will be required to develop a strategic plan every four years based on the council's risk profile to ensure that areas or activities with higher risks are audited over the longer term and that no higher risk area or activity is forgotten. This should align with the council's integrated planning and reporting framework and timetable.

The four-year strategic plan is to be developed in consultation with the Audit, Risk and Improvement Committee, governing body, general manager and senior managers. Final approval is to be given by the Committee.

The purpose of the plan is to decide and outline what council areas or activities will be covered in any given year, and if the area/activity is not covered in a given year, when it will be scheduled for review during the four-year period. It is to include:

- a description of the goals/objectives of internal audit
- key organisational issues and risks faced by the council, in order of priority, and
- which council areas will be audited over the four years, prioritised according to risk.

The Chief Audit Executive is to review and update the four-year strategic plan at least annually to ensure that it still aligns with the council's risk profile. This will also ensure that the council remains on track with its audits and any slippage in progress can be quickly addressed.

(b) The Chief Audit Executive is to develop an annual risk-based internal audit work plan, based on the strategic plan, to guide the council's audits each year in consultation with the governing body, general manager and senior managers. The work plan is to be approved by the Audit, Risk and Improvement Committee

The Chief Audit Executive will be required to develop an annual risk-based work plan for the council's internal audits based on:

- the priorities set by the council's four-year internal audit strategic plan
- the council's strategic goals and objectives, developed through the integrated planning and reporting framework
- the information obtained as part of the council's risk assessment process and the council's material risks
- any findings or risks raised by the NSW Auditor-General in its external audits of the council and sector-wide performance audits
- external factors such as industry trends or emerging issues, and
- any special requirements of the Audit, Risk and Improvement Committee.

The annual work plan is to be developed in consultation with the Audit, Risk and Improvement Committee, governing body, general manager, and senior managers. Final approval is to be given by the Committee.

The annual work plan is to identify:

- the key risks facing the council
- the key goals and objectives of the proposed audits
- the audits that will be carried out during the year and rationale for selecting each, having regard to areas of most significant risk to achieving the council's strategic objectives
- the resources needed for each audit (for example, staffing, budget, technology), including any external expertise needed
- the timing and duration of each audit
- the performance measures that will be used to measure against goals and objectives (described below)
- any areas not included in the work plan, which in the opinion of the Chief Audit Executive, should be reviewed, and
- quality assurance activities (where applicable).

The annual work plan is to be flexible enough to allow the Chief Audit Executive to review and adjust it as necessary in response to any changes to the council's risks or operations. Significant changes are to be approved by the Audit, Risk and Improvement Committee.

(c) The Chief Audit Executive is to ensure performance against the annual and strategic plans can be assessed

To establish the quality assurance and improvement program and to collect the data and information required to review the council's internal audit activities:

- the Chief Audit Executive will need to ensure internal audit work plans have performance indicators that can be measured against goals and objectives[64], and
- the general manager will need to ensure that a data collection or performance management system is established and maintained to collect the data needed to measure the impact of the internal audit function.

Performance indicators are to be set annually by the Audit, Risk and Improvement Committee, in consultation with the Chief Audit Executive and the general manager of the council.

[64] *Internal Audit in Australia* published by The Institute of Internal Auditors - Australia (2016) lists a range of examples of performance indicators that councils could consider when selecting their performance indicators

Core requirement 6:
How to perform and report internal audits

Proposal

It is proposed that:

(a) the Chief Audit Executive is to ensure that the council's internal audits are performed in accordance with the IPPF and current Australian risk management standards (where applicable), and approved by the Audit, Risk and Improvement Committee

(b) the Chief Audit Executive is to develop policies and procedures to guide the operation of the internal audit function, including the performance of internal audits

(c) the Chief Audit Executive is to report internal audit findings and recommendations to the Audit, Risk and Improvement Committee. Each finding is to have a recommended remedial action and a response from the relevant senior manager/s, and

(d) all internal audit documentation is to remain the property of, and can be accessed by, the audited council, including where internal audit services are performed by an external provider. It can also be accessed by the Audit, Risk and Improvement Committee, external auditor and governing body of the council (by resolution).

Description

(a) The Chief Audit Executive is to ensure that the council's internal audits are performed in accordance with the IPPF and current Australian risk management standards (where applicable), and approved by the Audit, Risk and Improvement Committee

Each council's internal audits are to be performed in accordance with statutory requirements, and the IPPF (only where the IPPF does not conflict with statutory requirements).

The internal audit methodologies used (that is, the tools or techniques used by internal auditors to conduct internal audits and analyse the information or data obtained) are also to be approved by the Audit, Risk and Improvement Committee.

Where risk information or ratings are used during the internal audit process, they must be developed and applied consistent with current Australian risk management standards. This means the Chief Audit Executive is responsible for ensuring that any risk information used in internal audits or any risk ratings given to internal audit findings and recommendations (for example, the risk of not implementing a recommendation) must be developed and assigned in a way that complies with AS ISO 31000:2018 and is consistent with council's risk management framework.

Performing internal audits

The Chief Audit Executive will be responsible for approving the project plan for each internal audit, supervising how each internal audit is conducted, and for any significant judgements made throughout each internal audit (including those performed by an external provider).

Each audit undertaken is to consist of following steps:

- **planning the internal audit** – which includes:
  - preliminary research
  - defining the audit's scope and criteria
  - defining the audit's objectives
  - timing
  - audit budget, and
  - information needed to perform the audit (for example, access to people, documents, systems)
- **performing the internal audit** – is to consider:
  - the objectives and purpose of the activity being reviewed
  - any risks to these objectives and the effectiveness of existing controls
  - opportunities to improve the efficiency and effectiveness of the activity, how risks are managed and council's performance more broadly
- **documenting and reporting the internal audit** - which includes:
  - documenting the evidence collected and analysed
  - producing working papers to support the findings and recommendations made
  - writing an audit report, and
  - discussing internal audit results with relevant staff and management.

It is best practice that each internal audit report is to be appropriately supervised and approved by a person not conducting the audit to ensure its findings and recommendations are accurate. Larger councils that employ or contract more than one internal auditor are encouraged to embed this practice into their audit process.

(b) The Chief Audit Executive is to develop policies and procedures to guide the operation of the internal audit function, including the performance of internal audits

The Chief Audit Executive is to ensure that the council develops and maintains policies and procedures to guide the operation of the internal audit function and the performance of internal audits. These policies and procedures should address:

- the structure, resourcing and professional development of the internal audit function
- strategic and annual audit planning
- audit methodology
- audit reports
- ongoing monitoring and reporting
- conducting internal audits and the quality assurance and improvement program
- resolving differences in professional opinion/judgements regarding internal audits
- communication between the governing body of the council, Audit, Risk and Improvement Committee, general manager, Chief Audit Executive and council staff - particularly of non-compliance or sensitive information, and
- information management including document retention, security and access to audit reports.

The Audit, Risk and Improvement Committee is to review and provide advice to the general manager of the council on all internal audit policies and procedures before they are finalised.

Where the internal audit function is outsourced, the Chief Audit Executive will be required to ensure that the external provider is consulted in the development and/or maintenance of internal audit policies and procedures.

(c) The Chief Audit Executive is to report internal audit findings and recommendations to the Audit, Risk and Improvement Committee. Each finding is to have a recommended remedial action and a response from the relevant senior manager/s

The Chief Audit Executive will be required to report the findings and recommendations of internal audits to the Audit, Risk and Improvement Committee at the end of each audit.

Each internal audit report written must include:

- necessary background information, including the objective and scope of the audit
- the audit processes and methodology used
- findings and recommendations based on the audit's objectives, prioritised according to their level of risk
- recommended remedial actions to address problems identified, which:
  - are risk-rated (that is, clearly show the severity of risks identified by the audit, focus management attention on high risks that need prompt attention and allow resources to be first applied to high risks rather than low risks), and
  - have been agreed to by the general manager and responsible senior managers of the council.

The Chief Audit Executive will be responsible for ensuring that each internal audit report (or supporting working papers) contains sufficient information that would enable another internal or external auditor to reach the same conclusions.

A copy of each internal audit report is to be provided to the Audit, Risk and Improvement Committee at the Committee's next quarterly meeting, or distributed out-of-session before the next meeting.

The council's response to internal audit report recommendations

The Chief Audit Executive is to provide a draft of each report to the responsible senior manager/s so that a response to each recommendation from each relevant business unit can be included in the final report that is submitted to the Audit, Risk and Improvement Committee. The general manager will have a maximum of ten working days to approve and provide the council's response to the Committee.

Responsible senior managers will have the right to reject recommended corrective action/s on reasonable grounds, but must discuss their position with the Chief Audit Executive before finalising the council's position with the general manager. Reasons for rejecting the recommendation/s must be included in the final audit report.

For those recommendations that are accepted, responsible senior managers will be required to ensure that:

- an action plan is prepared for each recommendation that assigns responsibility for implementation to a council staff member/s and timeframes for implementation
- all corrective actions are implemented within proposed timeframes, and
- the Chief Audit Executive is provided regular updates, or as otherwise reasonably requested by the Chief Audit Executive, in relation to the implementation of the internal audit action plan.

Where corrective actions are not implemented within agreed timeframes, the Audit, Risk and Improvement Committee can invite the responsible senior manager to explain why implementation has not occurred and how the resulting risk is being addressed in the interim.

The Audit, Risk and Improvement Committee can raise any concerns it may have about the council's response to internal audit reports in the committee's quarterly report to the governing body.

(d) All internal audit documentation is to remain the property of, and can be accessed by, the audited council, including where internal audit services are performed by an external provider. It can also be accessed by the Audit, Risk and Improvement Committee, external auditor and the governing body of the council (by resolution)

The Chief Audit Executive will be responsible for ensuring internal audit information (in whatever form) is documented, retained and controlled in accordance with the council's policies and any legislative or IPPF requirements. Internal audit documentation includes any information or documents produced or obtained by council's internal audit function that relates to the internal audit activities of the council.

All audit documentation is to remain the property of the audited council and can be accessed by the audited council, the Audit, Risk and Improvement Committee and the external auditor. This includes where the internal audits are performed by an external provider. Authorised access to internal audit documents must be outlined in council's Internal Audit Charter.

The governing body can also request access to internal audit information via a resolution of the council. The Audit, Risk and Improvement Committee is to decide the governing body's request. Any disputes between the governing body and the committee are to be referred to the Office of Local Government for resolution.

Apart from external audit purposes, it is envisaged that internal audit reports will be for internal council use only, subject to the requirements of the *Government Information (Public Access) Act 2009*. Approval must be obtained from Chief Audit Executive or Audit, Risk and Improvement Committee before internal audit reports are provided to any other person or external party.

The Chief Audit Executive or the Audit, Risk and Improvement Committee must obtain approval from the general manager prior to releasing any internal audit documents to external parties.

The general manager's approval is not required where the information is being provided to an external oversight or investigative such as, but not limited to, the Office of Local Government, the Audit Office, the Independent Commission Against Corruption or the NSW Ombudsman, for the purposes of informing that agency of a matter that may warrant its attention.

Core requirement 7:
Undertake ongoing monitoring and reporting

Proposal

It is proposed that an ongoing monitoring and reporting system be established where the:

(a) Audit, Risk and Improvement Committee is advised at each quarterly meeting of the internal audits undertaken and progress made implementing corrective actions

(b) governing body of the council is advised after each quarterly meeting of the Audit, Risk and Improvement Committee of the internal audits undertaken and the progress made implementing corrective actions, and

(c) Audit, Risk and Improvement Committee can raise any concerns with the governing body of the council at any time through the Chair.

Description

(a) The Audit, Risk and Improvement Committee is to be advised at each quarterly meeting of the internal audits undertaken and progress made implementing corrective actions

Ongoing monitoring and reporting to the Audit, Risk and Improvement Committee is essential to ensure that any emerging problems are identified and rectified quickly before their consequences escalate, especially in relation to material risks. It will also ensure that a clear message is sent that these matters are important and are being reviewed at the most senior levels in council.

To ensure this occurs, the Chief Audit Executive is to establish and maintain an ongoing monitoring system to track the internal audits undertaken within the council and follow-up the council's progress in implementing corrective actions. For smaller councils, this could simply be in a table or spreadsheet format.

The Chief Audit Executive is to ensure that the Audit, Risk and Improvement Committee is advised at each of the Committee's quarterly meetings of

- the number of internal audits completed during that quarter, including providing copies of the audit reports and advice on their findings
- progress in implementing the annual work plan
- progress made implementing corrective actions arising from any past internal audits, and
- any concerns the Chief Audit Executive may have.

The way this information is communicated is to be decided by the Audit, Risk and Improvement Committee in consultation with the Chief Audit Executive.

(b) The governing body of the council is to be advised after each quarterly meeting of the Audit, Risk and Improvement Committee of the internal audits undertaken and the progress made implementing corrective actions

Ongoing monitoring and reporting by the Audit, Risk and Improvement Committee to the governing body of the council is essential for accountability. It will also ensure that the governing body is kept abreast of the internal audits conducted and any emerging issues that may influence the strategic direction of the council or the achievement of the council's goals and objectives.

The governing body of the council is to be advised of the internal audits undertaken and progress made implementing corrective actions and any significant or emerging risk issues after each quarterly meeting of the Audit, Risk and Improvement Committee.

The governing body and the Audit, Risk and Improvement Committee is to decide how the Committee's advice is to be communicated. Options include providing the governing body with:

- a formal monitoring report from the Committee – this report would be for information only and a decision at the council meeting would not be required
- copies of the minutes of the Audit, Risk and Improvement Committee's meeting, or
- where appropriate, copies of the relevant agenda papers considered by the Committee at its quarterly meeting.

(c) The Audit, Risk and Improvement Committee can raise any concerns with the governing body of the council at any time through the Chair

Where the Audit, Risk and Improvement Committee is concerned about the progress of implementing corrective actions, or an internal audit-related issue arises, the Committee will be able to provide an additional report to the governing body of the council. This will ensure that the governing body is fully aware of the risks posed to the council.

The Chair of the Audit, Risk and Improvement Committee can also request at any time a meeting with the governing body of the council to discuss an internal audit-related issue.

Similarly, the governing body of the council can request by resolution at any time to meet with the Chair of the Audit, Risk and Improvement Committee regarding an internal audit-related issue.