The Institute of
Internal Auditors
Australia

4 April 2022

Mr Kym Della-Torre
Director, Advisory and Professional Development
Financial Management, Reporting and Policy Branch
Department of Treasury and Finance
200 Victoria Square
ADELAIDE, SA 5000

Email: apd@sa.gov.au

Dear Kym,

Please find our comments in relation to South Australian Treasury's proposal to replace Treasury Instructions 2 and 28 with a single new Treasurer's Instructions 2 - Financial and Risk Management.

Your sincerely

Peter Jones
Chief Executive Officer

Relationship to other Authoritative Guidance

Aspects of this exposure draft are inconsistent with the provisions of AS ISO 31000-2018, some are inconsistent with the SA Government Risk Management Guide published by SAFA.

In particular:

The concept of a "risk management plan" as a stand-alone document within an organisation is inconsistent with ISO 31000 and with the SAFA guidelines. An "annual risk management plan" is even further from the concepts of these documents.
The Standard allows that an organisation may develop a plan for the implementation of a risk management framework, but all other uses of the word plan relate to risk treatments or process improvements and do not describe a consolidated "risk management plan".

An organisation may have a series of inter-related plans that help it manage its risk. Such plans should be integrated with strategic/operational and other plans as is described in the SAFA document. That is, they should not be separate entities but should be an integral component of all other plans.

Consistent with ISO 31000 and the SAFA document, risk management is directed at creating and protecting value – achieving the objectives of the organisation. The exposure draft is directed at "mitigating" adverse outcomes. This ignores the "creating" part of the purpose of risk management. The guidance should use the term "manage" rather than "mitigate".

Professional Guidance

The exposure draft mentions having regard to professional guidance.

There is only one set of professional standards applicable to all aspects of internal auditing. This guidance is the *International Standards for the Professional Practice of Internal Auditing* issued by the *International Internal Auditing Standards Board*. This is a body sponsored by the Institute of Internal Auditors (The IIA) which operates independently of The IIA and is monitored by an oversight council composed of members of international organisations such as IFAC and the IMF.

The standards are published by The IIA within the *International Professional Practice Framework*. This document also contains a range of professional guidance applicable to the internal audit discipline.

In limited circumstances, the international standard ISO 19011 may be relevant and guidance issued by ISACA[1] or the AUASB[2] may be useful. However, it should be noted that the AUASB does not issue standards that are intended for application in the internal auditing environment.

---

1 ISACA (www.isaca.org) issues guidance for the conduct of the audits of information systems.

2 The Australian Auditing and Assurance Standards Board issues standards related to audits and reviews conducted under the Australian *Framework for Assurance Engagements*.

Level 5, 580 George Street, Sydney NSW 2000 | PO Box A2311, Sydney South NSW 1235
T +61 2 9267 9155 F +61 2 9264 9240 E enquiry@iia.org.au www.iia.org.au
ABN 80 001 797 557

Transitional and Pragmatic Issues

During a transitional period and for very small agencies it may be impractical to obtain completely "independent" members of an audit committee that is individuals who are not an employee of ***any*** State agency or authority. It might also not be possible in a very small agency for the governing body to appoint a senior officer of the agency to be the Chief Audit Executive. These and other issues of the kind should be addressed by a "comply or explain" policy.

Where, during a transitional period or to address particular issues related to the agency, the governing body cannot comply with the provisions of the Instruction, they should be required in their annual report to indicate this fact, to describe what they have done instead and to explain how the arrangements meet the purpose of the provision,

Comments in relation to specific sections

Section	Comment
4 (1)	The use of the word "mitigated" implies that risks are necessarily bad. This assumption is inconsistent with the Australian Standard on risk management (AS ISO 31000:2018). The word used should be "managed".
4 (2) (a)	The list of actions is inconsistent with the relevant guidance. Suggests that this section be rewritten as – "a risk management framework for the assessment, treatment, monitoring, and review of risks is established and maintained" Specifically the word "mitigating" should be removed as being inconsistent with the approach of relevant guidance.
4 (2) (b)	Is inconsistent with authoritative guidance (as described above). It is probably unnecessary but if a provision of this kind is sought, it should indicate that treatment plans must be integrated with plans for the delivery of the authority's services.
4 (3) (c)	The citation of the standard is incorrect. The standard is not a New Zealand standard. Correct citation is – "the Australian Standard AS ISO 31000:2018 *Risk Management – Guidelines*"
6 (3) (a)	Eight members is too many members for an audit committee. A more appropriate limit may be five.
6 (3) (c) and (d)	A better approach would be to prohibit any current employees of a South Australian public authority from serving on a public authority Audit and Risk Committee. (c) would become "must not have members that are employees of <u>any</u> public authority" (d) could be deleted.

Section	Comment
6 (4) (a)	An "annual risk management plan" is impractical and inconsistent with authoritative guidance. Replace with "management of risk within the authority".
6 (4) (b)	It would be more appropriate for the Audit and Risk Committee to approve the plan or to endorse it for approval by the governing body. Further, the concept of an "annual" internal audit work plan is not part of current internal audit discipline. An approved work plan is appropriate, but demanding it be established/approved annually is unnecessarily restrictive. There is no need for this document to prescribe a period. Suggest reword to: "reviewing and, if appropriate, endorsing for approval by the governing authority, the internal audit workplan prepared by the Internal Audit Executive"
6 (4) (f)	Repeats provisions already included at 6 (4) (b) and can be deleted.
7 (5)	This should be expanded to encompass ensuring adherence to professional standards as this is a primary responsibility of the head of function. A new paragraph at the beginning of the list should read – The internal audit function is conducted in a manner consistent with the *International Standards for the Professional Practice of Internal Auditing.*
7 (5) (a)	Given our comments at 6 (4) (b) this should read "...as approved by the Audit and Risk Committee".
7 (6)	As already discussed – remove the word "annual".
7 (6) (c)	This requirement may be resource intensive as it implies addressing all parts of the organisation over a three-year period. It also appears to be at variance with professional standards and good practice which require that internal audit planning be risk-based. Suggest that his provision be removed.
7 (7)	This should be explicit about the appropriate professional standards. It should also not concentrate on negative aspects of risk. While internal auditors should include action in response to the observations of the internal auditor, it may be best for the organisation if they are developed in association with management rather than (as implied here) imposed by the internal auditor. There is more to an internal audit report than "compliance". Suggest:

Section	Comment
	"Reports prepared by the internal audit function must have regard to professional guidance, such as the *International Professional Practices Framework* published by the Institute of Internal Auditors, and must include strategies to address any systematic faults".
11 (3)	Delete the definition of "annual risk management plan" as it will not be needed. Delete the work "annual" from "annual internal audit work plan" "compliance report" does not seem to be relevant to instruction 7. Does it refer to instruction 10? "internal control" has much wider application than financial risk. It may be best to quote the COSO definition from 1992 or to modify the entry to: "***internal control*** means rules, procedures, policies implemented by a public authority to ensure the achievement of objectives, compliance with regulatory requirements and integrity of reporting."