Standards Australia Limited
Exchange Centre, Level 10, 20 Bridge Street, Sydney New South Wales 2000
GPO Box 476, Sydney New South Wales 2001
Telephone +61 2 9237 6000, Facsimile +61 2 9237 6010
www.standards.org.au

4th November 2013

ASX Corporate Governance Council
Level 7, 20 Bridge St
Sydney NSW 2000
E: mavis.tan@asx.com.au

Dear Council Members

Corporate Governance Principles and Recommendations, draft 3rd Edition - Principle 7

These comments have been produced by the Risk Management Committee (OB7) of Standards Australia and Standards New Zealand in response to your request for comments on the draft third version of the ASX Corporate Governance Council's Corporate Governance Principles and Recommendations.

That committee is the custodian of the Australian and New Zealand risk management standard, AS/NZS ISO 31000 which has been adopted from the International standard. That standard was itself based on the earlier Australian and New Zealand standard, AS/NZS 4360.

AS/NZS ISO 31000 is the basis for risk management in most listed companies and other organisations in Australia and is the predominant and most widely adopted standard in the world.

The committee comprises representatives from a very wide range of stakeholder organisations, most of which have an intense interest in the application of risk management as part of an organisation's approach to governance. The members themselves have considerable experience in both governance and risk management as part of their employment. Their advice therefore reflects considerable practical experience in senior levels of organisations that are subject to the ASX Corporate Governance Council's Corporate Governance Principles and Recommendations.

In general, the committee applauds this revision of Principle 7 and the attempt to align it more closely with the Australian and international standard. Their suggestions therefore seek to clarify and simplify the terms used in the draft Principle, to reduce ambiguity, improve practicality, and improve alignment with modern-day concepts of risk and risk management.

I hope that the Corporate Governance Council finds these suggestions useful. The committee would be delighted to explain its advice in more detail and provide further input if required.

Yours sincerely

Bronwyn Evans

Dr Bronwyn Evans
Chief Executive Officer

Standards Australia's Risk Management Committee (OB7) Comments on Revised Principle 7 of the ASX Corporate Governance Council's Corporate Governance Principles and Recommendations

1. The revision from "system" to "framework" is to be applauded. However, the manner in which the term is used in parts of the draft Principle is inconsistent with the definition of framework given in the footnote to the Principle, as taken from AS/NZS ISO 31000. The framework for managing risk is the expression of the organisation's intentions for managing risk together with the arrangements that provide the required capacity to satisfy those intentions.

2. The term "material business risk" in meaningless in terms of the accepted definition of risk in the Australian and International standard as the *effect of uncertainty on objectives*. There is no reason to focus on "business risk", when the commentary to Recommendation 7.1 includes a very wide description of different types of risk and Recommendation 7.4 extends that range to economic, environmental and "social sustainability" risks

   The term "material" is not defined. This term is most often used to reflect significant weaknesses in an organisation's financial statements and its use in relation to risk is often construed to signal (again) that only those risks that are characterised by significant effects on financial performance are relevant.

   There is, moreover, a clear danger that important risks will be excluded from the Principle 7 processes because they are judged to be concerned with aspects other than 'business'.

   One of the purposes of the International standard is to harmonise the terminology of, and approaches to, risk management. Common terminology minimises misunderstanding and promotes efficient management. While we recognise that this term, like many others, is in common use we believe it is an unnecessary confusion of terminology and should be avoided.

   We recommend that the term "significant risk" is substituted for all occurrences of "material business risk".

3. The phrase "material business risk it is prepared to take to meet its strategic objectives" is meaningless in the light of the Australian and International definition of the word 'risk'. That phrase can be interpreted in an unnecessarily restrictive way. Risk is the effect on (all) objectives, not just those that the organisation mentions in its strategic plan. Those objectives are the overarching outcomes that the organisation is seeking. These are its highest expression of intent and purpose, and typically reflect its explicit and implicit goals, values and imperatives or relevant enabling legislation. Not all of these would be mentioned in its strategic plan or would be labelled 'strategic'.

   The Board should be interested in all the organisation's objectives and the risks to them - not just those within the strategic plan. For example, operational or compliance objectives will be of equal importance to the Board's considerations. It is therefore recommend that the term "strategic" be omitted.

4. The description of a framework to "identify, measure, monitor and manage risk on an ongoing basis" in several places confuses the purpose of the risk management *framework* (as defined in the footnote to Principle 7) with the risk

management *process*. It is recommended that this phrase be amended to "manage risk on an ongoing basis".

5. The phrase "identify, measure, monitor and manage risk on an ongoing basis" which is used throughout Principle 7 does not correctly describe the risk management process and is completely inconsistent with the Australian and International standard. It seems to be derived, in part, from a document of US origin.

   Risk management is a process of seven discrete steps and, critically, includes steps for identifying risk and also for the monitoring of risk and controls. The term "measuring" omits the most important purpose of risk analyses to develop an understanding of the risk. The phrase also omits the critical steps of communication and consultation (with stakeholders), establishing the context (defining scope and objectives and understanding the risk sources), risk evaluation (when a decision on the acceptability of risk is made) and risk treatment. This phrase should therefore be revised to either, simply, "manage risk" or to use a full description of the process for managing risk in terms of "consultation and communication, establishing the context, risk identification, risk analysis, risk evaluation, risk treatment and monitoring and reviewing".

6. The concept of a "risk culture" is a highly contentious issue where there is no accepted conclusion. The term is not defined and its use is ambiguous and generally inconsistent with the definition of risk. It is not part of the Australian and International standard.

   If the primary requirement for effective risk management is its complete absorption into and integration with an organisation's system of management, one aspect of that 'system' cannot have a separate culture from the rest: there can be only one culture for an organisation.

   It is strongly recommended that the requirement to "develop an appropriate risk culture" be omitted.

7. "Risk appetite" is also a much confused and often confusing concept. If the term is used here, it must be clearly defined. The international definition is "the amount and type of risk than an organisation is willing to pursue or retain"[1]. Either this definition should be given or, preferably, to be consistent with the Australian and International standard, the term "criteria" should be substituted for the term "appetite".

8. It is not the normal role of an organisation's risk management function to "test and continually improve the entity's systems for identifying, measuring and monitoring risk and its integral controls to avoid or mitigate risk" as given in the seventh paragraph of the commentary under Principle 7.1. This is generally the role of internal audit; risk management functions outside those specialist assurance providers in financial services or trading sector organisations do <u>not</u> ordinarily test systems or controls. It is recommended that the phrase "a dedicated risk function" be changed to "another assurance provider".

9. The phrase "integral controls to avoid or mitigate risk" in the seventh paragraph of the commentary under Principle 7.1 is inconsistent with the Australian and International Standard and the concept of risk sources that are opportunities as explained in the second paragraph of the commentary to Principle 7.

---

[1] ISO Guide 73:2009, Risk Management Vocabulary, Clause 3.7.1.2.

Also, adding "integral" has no value or meaning in this context. Controls are the means the organisation adopts to modify risk; by definition they must be "integral". It is possible the intended word is "internal" but this is also an unnecessary qualification. It is recommended that this phase be revised and simplified to read "controls to modify risk".

10. The long list of 'types' of risk given in the sixth paragraph of the commentary to Principle 7.1 is confusing. It mixes up functional activities, risk sources, types of event and types of consequences. Many of the 'types' described overlap and are ambiguous and confusing.

    Including such a list may mean that organisations then believe that these are the only 'types' of risk they should be concerned with and therefore unnecessarily restrict their approach to risk management and oversight. It is recommended that the second sentence of the sixth paragraph to Principle 7.1 be deleted entirely.

11. The phrase "Benchmarks they use to measure risk" in paragraph 8 of the commentary under Principle 7.1 is confusing. Organisations use 'criteria' as the basis for the analysis and evaluation of risk. "Benchmarks" are normally only used in the context of evaluating the relative effectiveness of all or part of an organisation's framework for managing risk. It is recommended that the phrase be revised to read "criteria used to analyse and evaluate risk". This phrase is consistent with the Australian and International standard.

12. The term "internal and external risks" in the ninth paragraph of the commentary under Principle 7.1 is incorrect. Risk is the "effect of uncertainty on objectives". Risk sources can be external or internal but risks are always "internal" as they are those that pertain to a particular organisation's objectives. It is recommended that this phrase be amended to read "internal and external risk sources".

13. The phrase "risk manifests itself" as used in the ninth paragraph of the commentary under Principle 7.1 is incorrect and confused. The term confuses events and their consequences with risk.

    Risk is the effect of uncertainty on objectives, it cannot "manifest itself". The correct terminology would be "If a significant event occurs...".

14. The term "economic, environmental and social sustainability risks" used in Recommendation 7.4 is ambiguous. For example, 'environment' can include the operating, political or legal environment. Similarly 'sustainability' can apply to a wide range of factors from the environment or to a natural resource such as a mineral deposit. It is recommended that these terms be either tightly defined to avoid confusion, wasted effort and the misinformation for stakeholders, or omitted.