Australian Government
Comcover

01 FACT SHEET

AS/NZS ISO 31000:2009

Risk Management – Principles and Guidelines

August 2010

Introduction

In November 2009, AS/NZS ISO 31000: 2009 replaced the previous Australian and New Zealand risk management standard AS/NZS 4360: 2004. AS/NZS ISO 31000:2009 (the Standard) provides Fund Member agencies with principles and general guidelines to be considered when developing risk management frameworks and programs. The Standard is supported by the:

- International Standard ISO/IEC 31010:2009–Risk Management;
- IEC/FDIS 31010 Risk Management–Risk Assessment Techniques; and
- ISO Guide 73:2009–Risk Management–Vocabulary.

This factsheet highlights some of the significant changes or enhancements of AS/NZS ISO 31000:2009. These include:

1. A change to the definition of risk;
2. The introduction of eleven principles for the management of risk;
3. Five attributes of an enhanced risk management framework; and
4. A recommended approach to developing an enterprise-wide risk management framework.

1. The definition of risk – 'the effect of uncertainty on objectives'

The definition of risk has changed from 'the chance of something happening that will have an impact on objectives' to ***'the effect of uncertainty on objectives'.***

While risk managers will continue to consider the possibility of risks occurring, they should now apply risk treatment options to ensure that the uncertainty of their agency meeting its objectives will be avoided, reduced, removed or modified and/or retained.

2. The introduction of the 11 Principles of risk management

1. Creates and protects value

Good risk management contributes to the achievement of an agency's objectives through the continuous review of its processes and systems.

2. Be an integral part of organisational processes

Risk management needs to be integrated with an agency's governance framework and become a part of its planning processes, at both the operational and strategic level.

3. Be part of decision making

The process of risk management assists decision makers to make informed choices, identify priorities and select the most appropriate action.

4. Explicitly address uncertainty

By identifying potential risks, agencies can implement controls and treatments to maximise the chance of gain while minimising the chance of loss.

5. Be systematic, structured and timely

The process of risk management should be consistent across an agency to ensure efficiency, consistency and the reliability of results.

6. Based on the best available information

To effectively manage risk it is important to understand and consider all available information relevant to an activity and to be aware that there may be limitations on that information. It is then important to understand how all this information informs the risk management process.

7. Be tailored

An agency's risk management framework needs to include its risk profile, as well as take into consideration its internal and external operating environment.

8. Take into account human and cultural factors

Risk management needs to recognise the contribution that people and culture have on achieving an agency's objectives.

9. Be transparent and inclusive

Engaging stakeholders, both internal and external, throughout the risk management process recognises that communication and consultation is key to identifying, analysing and monitoring risk.

10. Be dynamic, iterative and responsive to change

The process of managing risk needs to be flexible. The challenging environment we operate in requires agencies to consider the context for managing risk as well as continuing to identify new risks that emerge, and make allowances for those risks that no longer exist.

11. Facilitate the continual improvement of organisations

Agencies with a mature risk management culture are those that have invested resources over time and are able to demonstrate the continual achievement of their objectives.

3. Five Attributes to enhance risk management

1. An agency should fully accept accountability for their risks and develop comprehensive controls and treatment strategies.
2. There is now an increased emphasis on continuous improvement in risk management. Agencies should set its performance goals, its measures, and then review and modify processes as required. An agency should also review and modify its systems, resources and capability/skills to ensure continuous improvement.
3. Individuals with accountability for risk management are identified. These individuals should be appropriately skilled, have adequate resources to check and improve controls, monitor risks, and the ability to communicate effectively with all stakeholders.
4. Decision making within the agency, whatever the level of importance and significance, should include consideration of risks and the application of the risk management process as appropriate.
5. Frequent reporting to all stakeholders of the agency's risk management performance should be included in the agencies governance processes. This reporting would be ongoing and highly visible.

4. Developing an Enterprise-wide Risk Management Framework

The Standard outlines an approach to developing a framework that will assist agencies to integrate risk management into their enterprise-wide risk management systems. Agencies are encouraged to consider the links between the foundations of their risk management framework and their organisation objectives.

An agency's risk management framework needs to include its policy objectives and its commitment to risk management alongside its legislative responsibility. The risk management framework should be embedded within the agency's overall strategic and operational policies and practices, and take into consideration internal and external relationships, accountabilities, resources, processes and activities.

Strategic objectives

Senior Executives within an agency are responsible for providing the strategic direction of the agency. This approach, while usually long term, describes the vision for the management of risk and what overarching outcomes will be achieved.

Operational objectives

Generally, it is the middle managers of an agency who are responsible for aligning the strategic objectives with the agencies operations in order to achieve outcomes. The strategic plans developed at this level outline what each business unit must do to achieve their outcomes.

Line objectives

Similarly, line managers are responsible for developing strategic plans that are more specific to achieving outcomes and are short term in nature. These plans prescribe in detail how the processes or activities of the agency's outcomes will be actioned and completed.

References

1. International Electrotechnical Commission, *International Standard, ISO/ IEC 31010:2009, First Edition*, 2009.
2. Standards Australia/Standards New Zealand Standard Committee, *AS/NZS ISO 31000:2009, Risk Management-Principles and Guidelines*, November 2009.
3. International Organisation for Standardisation, *ISO Guide 73:2009, Risk Management-Vocabulary, First Edition*, 2009.
4. KNIGHT, Kevin W. 2009. Comcover Insurance and Risk Management Conference. *Transitioning to the new risk management standard AS/NZS/ISO 31000:2009*. 27 August. Canberra: Comcover, Department of Finance and Deregulation.