The Association of Insurance & Risk Managers
6 Lloyds Avenue
London EC3N 3AX
Tel: 0207 480 7610 Fax: 0207 702 3752 Email: enquiries@airmic.co.uk

An overview comparison of the AIRMIC/ALARM/ IRM Risk Management Standard with: -

- the Australia /New Zealand Standard AS/NZS 4360:2004
- the COSO Enterprise Risk Management - Integrated Framework

May 2005

1. Introduction

The Risk Management Standard developed by AIRMIC, IRM and ALARM has been compared with the Australia / New Zealand Standard (AS/NZS 4360:2004 and the COSO Enterprise Risk Management - Integrated Framework. The comparison is set out in tabular format with a summary of key points followed by more detailed comments on each main section of the Standards and how they compare.

At a ''high level'', all three documents are similar in that each of them: -

- sets out a generic ''process'' for risk management and accepts that there needs to be flexibility in implementation
- is applicable to a wide range of organisations and activities
- recognises that management of risk is part of good management practice, should be continuous and is best embedded into existing practices / business processes.
- recognises that there can be positive outcomes as well as negative outcomes
- sets out steps in the risk management process with brief guidance on each. (In the case of the Australia/ New Zealand and COSO documents, a second volume provides much more detailed guidance on the implementation of each step.)
- defines the terminology used

The comparison table takes each main element of the AIRMIC/IRM/ALARM Standard and comments on the comparable section in the other documents or how a particular topic is addressed if there is no exactly comparable section. It also comments on additional material in the more detailed AS/NZS and COSO documents that is not part of the AIRMIC/IRM/ALARM Standard.

All three ''Standards'' provide useful frameworks for risk management and guidance on implementation. Those familiar with the AIRMIC/IRM/ALARM Standard or applying it for the first time, may find it helpful also to refer to the other documents for additional information or a different perspective on a particular aspect of the risk management process.
In the next sections, we have indicated some of the material in the AS/NZS and COSO documents that adds to the AIRMIC/IRM/ALARM Standard and may be helpful in developing a comprehensive approach to risk management.

2. Business Objectives and Objective Setting

The AIRMIC/IRM/ALARM standard stresses the importance of relating risk management to the organisation's strategic and operational objectives and the threats / opportunities related to achieving those objectives. AS/NZS states that the first step in establishing the context within which an organisation operates is to establish the organisation's objectives and the internal and external environment in which the objectives are pursued.

COSO includes ''objective setting'' as one key component of its risk management process, making it clear that objective setting is a precondition to event identification, risk assessment and risk response*. '' There must first be objectives before management can identify and assess risks to their achievement and necessary actions to manage the risks''*
It identifies four key categories of objectives: -

- Strategic – the high level goals, aligned with supporting the organisation's vision. These reflect management's choice as to how the organisation will aim to create value for stakeholders.
- Operations – the objectives relating to the effectiveness and efficiency of the organisation's operations, including performance / profitability goals and safeguarding against loss.
- Reporting – the objectives relating to achieving reliable reporting both internal and external to the organisation.
- Compliance – the objectives relating to meeting the requirements of relevant laws and regulations. These requirements may relate to trade, pricing, taxes, environment, employee welfare, etc., and an organisation's compliance record can have a significant effect on its reputation.

COSO refers to the operations, reporting and compliance objectives as ''related objectives'' as they support and are aligned to the strategy of the organisation. It also points out that objectives in one category my overlap with or support objectives in another category.
COSO also draws a distinction between objectives whose achievement is not solely under the organisation's control and those where the organisation has control over its ability to do what is needed. Achievement of strategic and operations objectives may be influenced by external factors/ events whereas achieving compliance and reporting objectives is largely within the organisation's control.
In the Application Techniques document COSO gives further guidance on setting strategic objectives and the use of risk assessment, at this stage, to help decide between different options. It presents illustrations of linkages between the organisation's mission / vision and its strategic and related objectives.
There is also a useful section on risk appetite with questions that management might ask when considering risk appetite.

3. Risk Assessment

The AIRMIC/IRM/ALARM standard establishes that the estimation of probability of occurrence and the possible consequences can be qualitative, semi quantitative or quantitative. It gives simple examples relating both to threats and opportunities.
AS/NZS expands on this and provides a list of pertinent information sources and techniques which can be used when assessing probability of occurrence and consequences. In the Guidelines Document AS/NZS provides much more information on the following: -

- The choice of analysis method, which will be influenced by the context, the objectives and the resources that can be applied to the analysis.
  Types of risk measurement scales are discussed and examples of graphical representation of likelihood and consequence are given.
- Consequence and likelihood tables. These express different levels of severity for different types of consequence such as profit reduction, environmental impact, reputation impact, legal/regulatory impact, etc.
  Tables of likelihood also illustrate different levels of likelihood in terms of frequencies and simply in descriptive terms.
- The level of risk. AS/NZS shows how the level of risk can be described, depending on the type of analysis that has been undertaken.
- How opportunities can be analysed. Different levels of opportunity and how these can be presented are shown.
- Key questions that can be asked when analysing risks.

COSO too expands on the methodology for assessing risks both qualitatively and quantitatively. In the Application Techniques document COSO provides a useful description of how ‘’value at risk’’ models can be used, using illustrations of market value at risk, cash flow at risk, earnings at risk, etc. It also addresses sensitivity analysis and scenario analysis.
COSO provides examples of different ways of portraying risk assessment results including, risk maps, risk matrices using mean values of likelihood and impact, and risk matrices showing the variability in likelihood and impact.

The AIRMIC/IRM/ALARM standard indicates that risk treatment includes control / mitigation as a major element, but also extends to risk avoidance, risk transfer, risk financing, etc. It also stresses the need to evaluate the cost – effectiveness of any proposed risk treatment measures.

AS/NZS provides more detail and deals separately with options for treatment of risks with positive outcomes versus treatment of risks with negative outcomes. It identifies options for treatment of risks with positive outcomes as including: -

- Actively seeking an opportunity by deciding to start or continue an activity which is likely to create the opportunity

4. Risk Treatment

- Changing the likelihood of the opportunity
- Changing the consequences to increase the extent of the gains
- Sharing the opportunity with other parties in order to increase the likelihood and / or the gain.
- Retaining the opportunity without any immediate action being required.

In the case of risks with negative outcomes, AS/NZS identifies similar types of treatment options as follows: -

- Avoiding the risk by deciding not to start or continue with an activity
- Changing the likelihood of negative outcomes
- Changing the consequences to reduce the extent of losses.
- Sharing the risk via contracts, insurance, etc., in order to transfer liability
- Retaining the risk.

In the Guidelines document AS/NZS provides more information on treatment options including crisis/ business continuity plans, contracting and insurance.
It sets out guidance on designing risk treatment options and the trade- off between costs and benefits. It describes a qualitative approach to cost benefit analysis as well as a quantitative approach. Finally it stresses the importance of risk treatment plans which should: -

- Identify responsibilities, schedules, budgets, performance measures and expected outcomes of risk treatment.
- Include mechanisms for assessing and monitoring treatment effectiveness against treatment objectives
- Document how the chosen options will be implemented.

In its section on risk response, COSO introduces the portfolio, or entity wide, perspective of risk. For example, the risks in different business units of a major company may be within the risk tolerance levels of those business units, but taken together, these risks may exceed the risk appetite of the company as a whole. In the Application Techniques, COSO gives further detail on: -

- Linking risk response to objectives, events and risk assessment
- The effect of risk response on residual risk

5. Limitations of Enterprise Risk Management

- Multiple risk responses
- Cost – benefit analysis of alternative risk response
- Further information on the portfolio view of residual risk

COSO contains a section on the limitations of enterprise risk management. It points out that no matter how well designed and implemented, ERM can only provide reasonable assurance to the management and the Board of Directors that the organisation's objectives will be achieved.

It identifies three important issues that need to be recognised: -

- Risk relates to the future which is inherently uncertain
- Enterprise risk management, however effective, operates at different levels with respect to different objectives. It can help ensure that management is aware of the extent to which the organisation is moving toward achievement of its objectives. It cannot provide assurance that the objectives will be achieved.
- Enterprise risk management cannot provide absolute assurance with respect to any of the assurance categories.

The section identifies ways in which a well designed risk management system can break down which include human judgment, human errors caused by carelessness, distraction or fatigue, collusion between two or more individuals and the deliberate over riding of policies / procedures by management.

airmic

An overview comparison of the AIRMIC/ALARM/ IRM Risk Management Standard with the Australia /New Zealand Standard and the COSO Enterprise Risk Management - Integrated Framework

A Risk Management Standard AIRMIC / ALARM / IRM 2002	Australian/New Zealand Standard AS/NZS 4360: 2004	Enterprise Risk Management – Integrated Framework COSO 2004
Summary A short 14-page document which sets out the ''standard'' with the terminology definitions as an appendix.	**Summary** A 30 page document setting out the ''standard'' with a companion volume (109 pages) setting out Risk Management Guidelines. The most recent of the three documents.	**Summary** A 125-page document sets out an executive summary (7pages) followed by a detailed description of the Risk Management Framework. A second volume (105 pages) provides ''Application Techniques'' with detailed guidance and examples.
Sets out a generic process for risk management, applicable to a wide range of organisations / activities.	Standard sets out a generic process for risk management which is independent of any specific industry or economic sector.	Sets out a generic risk management process with more emphasis on ''business risk'', value creation and internal control.
Recognises there is an ''upside'' to risk as well as a ''downside'', but addresses mainly the ''downside''.	Recognises ''upside'' and ''downside'' of risk, referring to ''potential gains'' and ''potential losses'' and to ''positive and negative outcomes''. Addresses both, in parts of the standard eg Risk Treatment.	Recognises ''upside'' and ''downside'' of risk, expressing this more in terms of uncertainty and the associated risks and opportunities.
Sets out steps in the risk management process with very brief guidance on each.	Sets out process and brief content for each step. The process is very similar to that in the AIRMIC Standard. Provides its own definitions of terms with reference to ISO definitions in some cases.	Sets out ''components of risk management'', ie the risk management process. Presents a three dimensional matrix to relate the organisations objectives to the risk management components and to the business unit structure of the organisation.
Follows the terminology for risk, set out in the ISO/IEC Guide 73 – Risk Management Vocabulary- Guidelines for use in Standards.		Provides a section on ''definition'' which contains significant discussion as well as defining key terms, such as enterprise risk management. It does not set out definitions of each term in the same way as the other two.

A Risk Management Standard AIRMIC / ALARM / IRM 2002	Australian/New Zealand Standard AS/NZS 4360: 2004	Enterprise Risk Management – Integrated Framework COSO 2004
Summary (continued)	**Summary (continued)** Companion volume – Risk Management Guidelines. Reproduces each section of the Standard and then expands on it with detailed guidance and examples.	**Summary (continued)** Companion volume – Application Techniques. Takes each component of risk management and gives detailed guidance and examples on how to implement each.

airmic

Detailed comparison of key elements of each approach

A Risk Management Standard AIRMIC / ALARM / IRM 2002	Australian/New Zealand Standard AS/NZS 4360: 2004	Enterprise Risk Management – Integrated Framework COSO 2004
Introduction Makes the point that standard is needed to ensure an agreed: - • use of terminology • process by which risk management is carried out • organisation structure for risk management • objective for risk management Establishes that standard is not prescriptive and that there is flexibility in meeting the component parts. Standard represents best practice against which organisations can measure themselves.	**Preface and Foreword** Comparable to AIRMIC introduction and COSO Foreword. Only document that is a revision of an earlier Standard (1995 and revised 1999) Intention is to provide generic framework with more emphasis on: - • embedding risk management practices in an organisations culture • risk as an exposure to the consequences of uncertainty and potential deviations from what is planned/expected. • managing potential gains as well as potential losses. • Guidance and examples provided in a new handbook.	**Foreword** Comparable to AIRMIC Introduction. Refers to earlier document; Internal Control – Integrated Framework. Expresses the need for an enterprise risk management framework: - • providing key principles/concepts • a common language • clear direction and guidance Expands on, but does not replace, the earlier internal control document which is incorporated in this wider enterprise risk management framework. Organisations can use this framework to move to a fuller risk management process.
Risk Standard defines risk (as per ISO/IEC guide 73) Definition of all other terms is in the reproduction of ISO/IEC Guide 73 in the Appendix. Emphasises opportunities for benefit (upside) as well as threats to success (downside) Makes the point that safety risk is concerned only with the negative.	**Scope and General** AS/NZS defines risk in this section and also sets out all other definitions of terms. Definitions are AS/NZS own definitions with use of ISO terminology in some cases. Scope and general also has some further introduction setting out the objective of the standard and that it is not intended to enforce uniformity of risk management systems.	**Definition** The first main section in the framework document has substantial discussion of the key terms. Risk is defined as possibility of an event that will have an adverse effect on achieving objectives. Opportunity is defined as possibility of an event that will positively affect achievement of objectives.

airmic

Detailed comparison of key elements of each approach (continued)

A Risk Management Standard AIRMIC / ALARM / IRM 2002	Australian/New Zealand Standard AS/NZS 4360: 2004	Enterprise Risk Management – Integrated Framework COSO 2004
Risk Management Standard emphasises risk management as: - • central part of strategic management • a continuous and developing process • part the culture of the organisation • supporting operational efficiency at all levels Standard describes external and internal drivers of risk, categorising them as financial, strategic, hazard and operational. Standard sets out the basic risk management process diagram. Standard sets out benefits of risk management.	**Risk management process overview and Risk Management Context** Basic risk management process diagram is set out. This is very similar to the process set out in the AIRMIC standard. The ''context'' includes the organisation's internal and external environment and the interface between the two. The same concept as expressed in the AIRMIC diagram of external and internal drivers of risk and the interface between the two.	**Components of Risk Management** COSO does not have an exactly comparable section here, but discusses in a number of places: - • The link to business objectives • The organisation's internal environment • Four categories of objectives – strategic, operations, reporting and compliance • Risk management philosophy and risk appetite.
Objective Setting There is no specific section dealing with objective setting (as in COSO), but AIRMIC does stress the importance of relating risk management and risk assessment to strategic objectives.	**Objectives** Goals and objectives are addressed as part of establishing the risk management context.	**Objective setting** COSO has ''objective setting'' as one component of risk management. It emphasises strategic objectives as supporting the organisations vision and mission. Categories of ''related objectives'' are identified as Operations, Reporting and Compliance. This section also addresses achievement of objectives, risk appetite and risk tolerance of the organisation.

airmic

Detailed comparison of key elements of each approach (continued)

Risk Management Standard AIRMIC / ALARM / IRM 2002	Australian/New Zealand Standard AS/NZS 4360: 2004	Enterprise Risk Management – Integrated Framework COSO 2004
Risk Identification AIRMIC treats risk identification as part of risk analysis which also includes risk description and risk estimation. Guidance is very limited – risk identification should be done in a methodical way to ensure that all activities and all risks are defined. A short list of risk identification techniques is given in the appendix.	**Identify Risks** Very short section in which AS/NZS stresses need for systematic approach to identify risks, whether or not they are under the control of the organisation. The Risk Management Guidelines expand on the identification process, the information needed, the approaches to identifying risks and documentation of risk identification.	**Event Identification** COSO refers to ''events'' (external or internal) which affect implementation of strategy. Events may have positive or negative impact. Document lists external and internal influencing factors that drive events and event categories. (this appears comparable to the AIRMIC diagram of Drivers of Key Risks.) COSO gives more detail on event identification techniques in the framework document. The Application Techniques document provides a variety of examples with outlines for facilitated workshops, process flow analysis, questionnaires, etc.
Risk Description Deals briefly with structured format for recording the risks identified (with an example table)	**Documentation** Deals with recording the risk identification step (in the Guidelines) and gives examples of risk registers in Section 10 of the Guidelines – ''Recording the Risk Management Process''.	**Risk Description** COSO does not deal separately with recording risk identification, but incorporates it into the recording of risk assessment.

airmic

Detailed comparison of key elements of each approach (continued)

Risk Management Standard AIRMIC / ALARM / IRM 2002	Australian/New Zealand Standard AS/NZS 4360: 2004	Enterprise Risk Management – Integrated Framework COSO 2004
Risk Assessment AIRMIC uses ISO term ''risk estimation''. Gives simple tables of examples for assessing consequences and probability – for both threats and opportunities.	**Analyse Risks** AS/NZS addresses qualitative, semi-quantitative and quantitative estimation of consequences and likelihood. (and the need to take account of existing controls) It lists information sources and techniques for estimating consequences and likelihood. The Risk Assessment section of the Guidelines document is comprehensive. It shows a good spread of risk assessment approaches from the very simple to the more detailed quantitative. It also specifically addresses the analysis of opportunities.	**Risk Assessment** No significant differences from the other documents. COSO addresses inherent and residual risk. COSO discusses assessment techniques such as benchmarking, probabilistic and non-probabilistic methods. The Risk assessment section in the Application Techniques document is comprehensive. It tends to be more financially oriented with analyses of earnings at risk, cash flow at risk, value at risk, etc.
Risk Evaluation Very short section makes the point that after risk assessment, it is necessary to compare risks to risk criteria established by the organisation. Decisions about accepting or treating a risk should then be made.	**Risk Evaluation** AS/NZS has similar very short section. The Guidelines cover evaluation criteria, the concepts of tolerable risk and ''ALARP''. There is also reference to historical events in determining risk criteria.	**Risk Evaluation** No exactly comparable section. Some comments are incorporated in the Risk Assessment and Risk Response Sections.
Risk Reporting and Communication AIRMIC deals with reporting of risks internally and externally, before moving on to risk treatment.	**Risk Reporting and Communication** AS/NZS deals with communication and consultation separately at the start of the standard.	**Risk Reporting and Communication** COSO addresses information and communication after Risk Response and Control Activities.

airmic

Detailed comparison of key elements of each approach (continued)

Risk Management Standard AIRMIC / ALARM / IRM 2002	Australian/New Zealand Standard AS/NZS 4360: 2004	Enterprise Risk Management – Integrated Framework COSO 2004
Risk Treatment AIRMIC does not give much detail, but states that risk control/ mitigation is a major element of risk treatment which also extends to avoidance, risk transfer and risk financing. It addresses cost /effectiveness of risk treatment and that compliance with laws and regulations is not optional.	**Treat Risks** AS/NZS deals separately with options for treating risks with positive outcomes and for those with negative outcomes. It briefly refers to the cost / benefit analysis of treatment options. The Guidelines provide more information on treatment options, including sharing risk, contracting, insurance, contingency planning, etc. Guidelines also deal with selecting treatment options and cost / benefit analysis – both qualitative and quantitative.	**Risk Response** COSO deals with treatment options in four categories: - • Avoidance • Reduction • Sharing • Acceptance Framework document deals very briefly with cost / benefit analysis. The Applications techniques document provides more detail on risk responses and gives examples of tables recording actions, risk reduction, etc.
Monitoring and Review of Risk Management AIRMIC makes the point that monitoring should provide assurance that risks are identified and appropriate controls are in place.	**Monitor and Review** AS/ANZ indicates that ongoing review is essential and that lessons should be learned by reviewing events, treatment plans and their outcomes. Guidelines expand on this, dealing with assurance and monitoring, risk management performance measurement and post-event analysis.	**Monitoring** COSO separates monitoring into ongoing monitoring activities and separate evaluations. It deals with reporting in this section including what is reported and to whom.

Detailed comparison of key elements of each approach (continued)

Risk Management Standard AIRMIC / ALARM / IRM 2002	Australian/New Zealand Standard AS/NZS 4360: 2004	Enterprise Risk Management – Integrated Framework COSO 2004
Structure and Administration of Risk Management The standard sets out roles and responsibilities for: - • The Board • Business units • The Risk management Function • Internal Audit In addition it comments on Risk Management Policy and resources for Implementation.	**Establishing effective Risk Management** AS/ANZ deals more generally with this area and refers to: - • evaluating existing practices • Ensuring senior management support • Establishing accountability and authority • Ensuring adequate resources The Guidelines expand on this to some extent, but not significantly.	**Roles and Responsibilities.** COSO sets out roles and responsibilities for: - • The Board • Management • The Risk Officer • Financial Executives • Internal auditors • External parties The Application Techniques provide more detail including example role descriptions for the Chief Risk Officer, the CEO, the Audit Committee, the Risk Committee, etc.
(No equivalent to COSO Section)	. **(No equivalent to COSO Section)**	**Limitations of Enterprise Risk Management** COSO indicates that however good the risk management system, it can only provide reasonable assurance regarding achievement of objectives. Limitations include: - • Management processes • Human error/ mistakes • Deliberate circumventing of controls • Costs of risk responses • Etc.