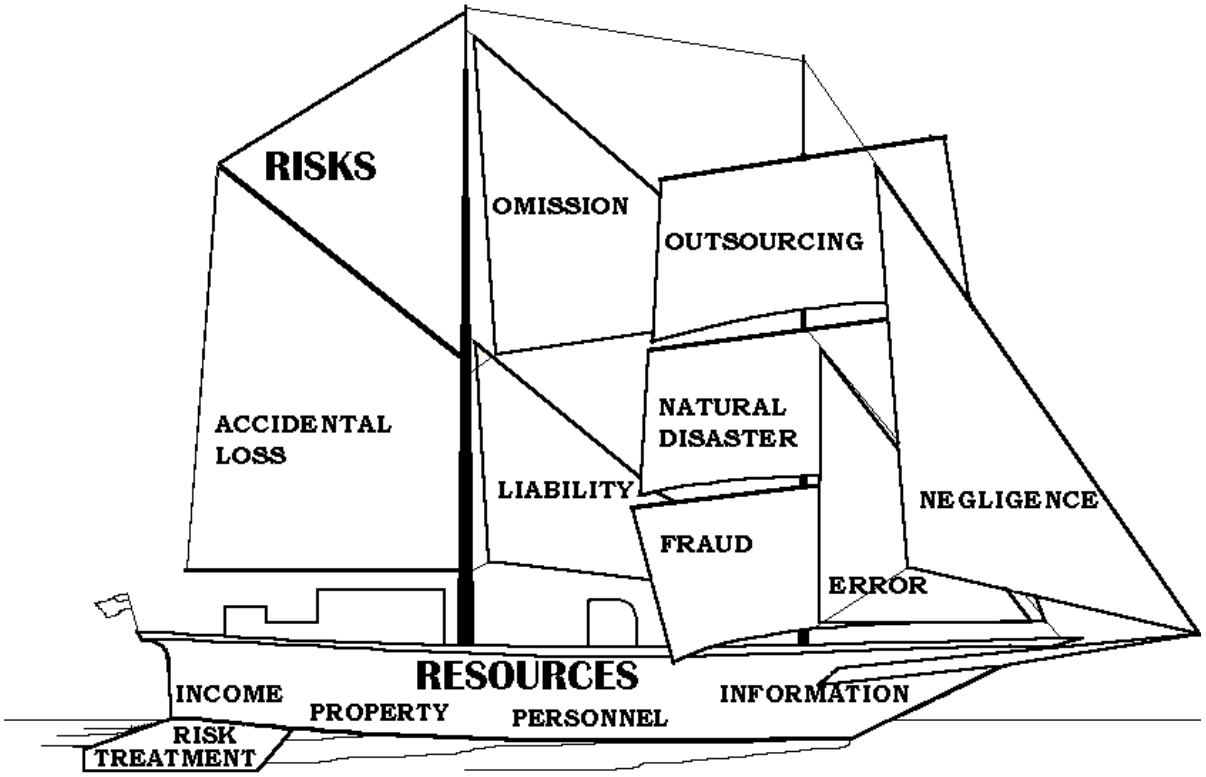
RISK MANAGEMENT

A JOURNEY.....



.....NOT A DESTINATION!

Kevin W. Knight AM
Chairman
ISO TMB Working Group on Risk Management
Member
Standards Australia/Standards New Zealand Joint Technical Committee
OB/7 – Risk Management

KEVIN W. KNIGHT AM
CPRM; Hon FRMIA; FIRM (UK); LMRMIA.
P O Box 226
NUNDAH Qld 4012
AUSTRALIA
Telephone: (+617) 3266 4661
E-mail: kknight@bigpond.net.au

June 2010

Kevin W Knight AM is well known through his very active work in explaining and encouraging the use of Standards with respect to the management of risk. He is a founding member of the Standards Australia/Standards New Zealand Joint Technical Committee that produced the original AS/NZS 4360 Risk Management Standard in 1995 and its subsequent revisions in 1999 and 2004. Kevin was Convenor of the International Organisation for Standardisation (ISO) Working Group that produced ISO/IEC Guide 73:2002 – RM Terminology and he currently Chairs the ISO Working Group that developed the new ISO 31000:2009 Risk Management Standard and the revised ISO Guide 73:2009 Risk Management Vocabulary.

Kevin has been very active in furthering the risk management profession and the professional development of its practitioners throughout the Asia - Pacific Region in particular, as well as globally, over the past 28 years. He has been widely published and quoted by the risk management media throughout the world as a leading proponent of the management of risk. He has presented papers, lectures, seminars and workshops on the application of Standards to the management of risk in Japan, Korea, China, Taiwan, The Philippines, Indonesia, Singapore, Malaysia, India, South Africa, Argentina, Brazil, USA, Canada, Belgium, Denmark, England, France, Ireland, Italy, Monaco, Poland, Romania, Spain, The Czech Republic and Wales in addition to his extensive activities in Australia and NZ.

In 1988 he identified the need for the development of appropriate professional training and education as one of the most urgent needs of the Asia-Pacific region. As a result he has been actively involved in the development of Risk Management Education syllabi that not only benefit Australian practitioners but are also relevant to the professional development of risk management practitioners throughout the Asia-Pacific region.

Kevin also recognised the need for greater unity of risk management practitioners if their voice was to be recognised and heeded by government and corporate decision makers. He has actively worked for over 30 years to achieve greater cooperation within not only the Australian risk management community but within Asia as well as globally. His work was recognised by his peers in 1996 when the Board of the International Federation of Risk & Insurance Management Associations presented him with an award ***in recognition and appreciation for outstanding contributions and leadership to IFRIMA*** and the Association of Risk & Insurance Managers of Australasia at its Annual General Meeting elected him an ***Honorary Life Member***. The Australasian Institute of Risk Management Annual General Meeting in 2000 elected him as an ***Honorary Fellow***.

He was the 2001 Asian Risk Manager of the Year. The citation accompanying the award noted his ***long-term commitment to the development of robust corporate cultures committed to strong risk management practices and procedures. His active involvement in assisting a wide range of organisations in the National, Regional and Local Government areas within Australia and New Zealand to adopt and develop effective risk management regimes and his work within Education Queensland in developing the application of risk management techniques to the management of students with behavioural problems due to intellectual and other difficulties*** was also noted.

In 2003, he was the recipient of the Standards Australia ***Outstanding Service Award (Committee Member)*** in recognition of his ***contribution to the development of Australian and International Standards for risk management, for the ultimate benefit of the Australian community*****.**

He was appointed a Member in the General Division of the Order of Australia by the Governor-General of Australia in 2008 ***"for service to risk management through executive roles with professional associations and as a contributor to the development of principles and practices"*****.**

Kevin was included in the US *Treasury & Risk's* Magazine 2008 list of the ***100 most influential people leaving their marks on the world of finance*** for his International Standards work.

Kevin spent over 25 years working in security and risk management roles for a number of Australian Government Departments and Authorities and 10 years with the Department of Education in the State of Queensland. He retired in 2004 and fills in his time in the following honorary activities:

- Chairman of the International Organisation for Standardisation (ISO) Working Group on Risk Management Standards;
- Member of the Standards Australia/Standards New Zealand Joint Technical Committee OB/7 - Risk Management;
- Risk management liaison member on the ISO Joint Technical Coordination Group
- Risk management liaison member on ISO Technical Committee 223 (Societal Security)
- External Member of the Risk Management Committee of the Senate of the University of Queensland;
- Member of the Academic Council of the Australian & New Zealand Institute of Insurance and Finance; and
- Adjunct Lecturer, Department of International Business & Asian Studies, Business School, Griffith University, Australia

To Laugh is to Risk

To laugh is to risk appearing the fool
To weep is to risk appearing sentimental
To expose feelings is to risk exposing your true self
To reach out to another is to risk involvement
To place your ideas, your dreams before a crowd is to risk their loss
To love is to risk not being loved in return
To live is to risk dying
To hope is to risk despair
To try is to risk failure.

But risks must be taken
because the greatest hazard in life is to risk nothing
The person who risks nothing, does nothing, has nothing, and is nothing.
They may avoid suffering and sorrow
but they cannot learn, feel, change, grow, love, live.
Chained in by their attitudes, they are a slave,
they have forfeited their freedom

Only the person who risks is free.

Anonymous

What are we up against?

Risk is an unsavoury topic — like incontinence, sewerage farms and colostomies — we don't want to talk about it.

The following quotes come to mind:

People don't want the truth, they just want comforting.

(Machiavelli)

'And beyond the wild wood?',* Mole asked Ratty. Ratty replied, *'Beyond the wild wood comes the wide world, and that's something that doesn't matter either to you or to me. Don't ever refer to it again please.'

('The Wind in the Willows')

We only think when we are confronted with a problem.

(John Dewey)

One little slip, Laura, that's all
Said right, meant left
One little word

(John Cleese as Mr Stimpson in 'Clockwise')

Evidently, part of the situation we need to deal with is common to all people — the desire to avoid unpleasantness — if necessary, by burying our heads in the sand.

Elementary, Dear Watson

Risk Management, at its most basic level, is all about common sense. Sometimes risk managers get so caught up in the intricacies that they miss the blatantly obvious, as illustrated here:

Sherlock Holmes and Dr Watson went on a camping trip. After a good meal and a bottle of wine they went to their tent to sleep. Some hours later, Holmes awoke and nudged his faithful friend.

"Watson, look up at the sky and tell me what you see."

Watson replied: *"I see millions and millions of stars."*

"What does that tell you?"

Watson pondered for a minute.

"Astronomically, it tells me that there are millions of galaxies and potentially billions of planets. Astrologically, I observe that Saturn is in Leo. Horologically, I deduce that the time is approximately quarter past three. Theologically, I can see that God is all powerful and that we are small and insignificant. Meteorologically, I suspect that we will have a beautiful day tomorrow. What does it tell you?"

Holmes was silent for a minute, then spoke.

"Watson you cretin. Some bounder has stolen our tent!"

The nicest thing about not planning is that failure comes as a complete surprise and is not preceded by a period of worry and depression.

John Preston, Boston College

Better to proceed in the knowledge of some of the risks rather than in complete ignorance.

Bernie Hough 1985

How Did We Survive?

Looking back, it's hard to believe that we have lived as long as we have.

As children we would ride in cars with no seat belts or air bags.

Riding in the back of a Ute or truck on a warm day was always a special treat.

Our baby cribs were painted with bright coloured lead based paint. We often chewed on the crib, ingesting the paint.

We had no childproof lids on medicine bottles, doors, or cabinets, and when we rode our bikes we had no helmets.

We drank water from the garden hose and not from a bottle. We would spend hours building our go-carts out of scraps and then rode them down the hill; only to find out we forgot the brakes. After running into the bushes a few times we learned to solve the problem.

We would leave home in the morning and play all day, as long as we were back when the streetlights came on. No one was able to reach us all day. (Kids now ALL carry mobile phones!!!)

We played brandy and other ball games and sometimes the ball would really hurt.

We ate cupcakes, bread and butter, and drank spiders and floaters, but we were never overweight; we were always outside playing.

Basketball, football and cricket had tryouts and not everyone made the team. Those who didn't had to learn to deal with disappointment.

Some students weren't as smart as others so they failed a grade and were held back to repeat the same grade.

That generation produced some of the greatest risk-takers and problem solvers. We had the freedom, failure, success and responsibility, and we learned how to deal with it all.

The greatest risk of all is to take no risk at all. Without risk there is no advancement. The challenge for us all is to manage the risk so as to ensure a successful outcome.

(Anon)

Linking risk management to assurance

Systems to monitor and review risks and the risk management process require careful selection, targeting and planning as they absorb scarce resources. Priority should be given to:

- high exposure risks, that is, where the consequence of the event could be high;
- high current residual risks, where there is evidence of low control effectiveness;
- the potential for failure of controls, especially where this would result in high, or frequent, consequences;
- activities where change could give rise to significant risk;
- parts of the organisation that are consciously exposed to high levels of risk;
- technological advances that may offer more effective or lower cost alternatives to current risk treatment.

In general terms, monitoring and review practices will be of one of three types:

- Continuous (or at least frequent) monitoring through routinely measuring or checking particular parameters (for example pollution levels, or cash flows).
- Line management reviews of risks and their treatments – Control Self-Assessments, Quality reviews etc - which are often selective in scope but typically routine and regular and which should be selected on risk-weighted criteria.
- Independent review – using both internal and external audit staff. As far as possible these should test systems rather than conditions. They will be more selective in scope and lower frequency than the above measures. If audits become or are seen as being the primary system of assurance, then it is axiomatic that the assurance regime will be weak.

SAA HB 158—2006 Delivering assurance based on AS/NZS 4360:2004 Risk Management

Internal audit involvement in risk management

It is not uncommon for the internal audit function of an organisation to work in close cooperation with the risk management function. Some organisations do not have a formal risk management function and in this case the internal audit often provides risk management consulting services to the organisation.

Internal audit may provide risk management consulting if certain conditions apply:

• It should be clear that management remains responsible for risk management. Internal audit should not manage any risks on behalf of management. Whenever internal audit acts to help the management team to set up or to improve risk management processes, its plan of work should include a clear strategy and timeline for migrating the responsibility for these activities to members of the management team.*****

• The nature of internal audit's responsibilities should be documented in the audit charter and approved by the Audit Committee. Any work beyond the assurance activities should be recognised as a consulting engagement and the implementation standards related to such engagements should be followed. #

• Internal audit should provide advice, challenge and support to management's decision making, as opposed to taking risk management decisions themselves. Internal audit cannot give objective assurance on any part of the risk management framework for which it is responsible. Such assurance should be provided by other suitably qualified parties.

**** IIA-UK ERM Position Statement***
 # IIA Professional Practices Framework and IIA-UK ERM Position Statement

SAA HB 158-2006 Delivering assurance based on AS/NZS 4360:2004 – Risk Management

Perspectives on the management of risk

Enterprises with a commitment to managing risk are generally more open to the adoption of standards such as ISO 31000, ISO 9000 (quality management), ISO 14001 (environmental management) and ISO 15489 (records management) when they are shown how adopting standards, in full or in part, can enable them to manage risk more effectively and therefore maximize opportunities in order to achieve corporate objectives.

Management of risk is an integral part of good management. It is an iterative process of continual improvement that is best embedded into existing practices or business processes.

An effective risk management regime is a combination of the culture, processes and structures that are directed towards realising potential opportunities whilst managing adverse effects.

An organization's culture is the sum of its people, symbols, stories, business experiences, power structures, control systems, organizational structures, rituals and routines that, when combined, make it unique.

The management system adopted must ensure that all risks have owners who have accountability for their management and who also have the authority and resources to make decisions with respect to the treatment of the risk.

Risk management practitioners are often their own worst enemy when it comes to championing the cultural change required in an organization if it is to effectively manage its risks.

Sadly, this is not a recent phenomenon as the following quote from Felix Kloman, a long-time commentator, prophet and philosopher on risk management and the management of risk illustrates. His comment in *"The Revolt of the Risk Manager",* published in *Bests Review*, October 1971, is as fresh and applicable today as when first made 37 years ago:

> *Until the Risk Manager can be completely free of his real and psychological ties to insurance and the insurance industry, he will not be able to perform the risk management function.*

The challenge facing today's risk management practitioner is not just breaking free of the mantra that *"risk management is all about insurance, and if we have insurance, then we have managed our risks"*, but rather being accepted as a provider of professional advice and service to the risk makers and the risk takers at all levels within an organisation. It is the risk makers and the risk takers who must be the owners of risk and accountable for its effective management.

A consequence of the uncertainty as to the place of risk management in an organization and the role of the risk practitioner has seen a plethora of persons and professional bodies presenting themselves as the true "risk managers".

The accounting and audit bodies are the latest to set themselves up as the arbiters of risk management through their active involvement in the development and promulgation of the framework document from the Committee of Sponsoring Organizations of the Treadway Commission (COSO) in the USA with its heavy accounting, financial management and audit bias.

Those seeking to find the most useful processes and guidance on risk management are continually faced with the difficult task of deciding what to recommend to Boards and executive management.

In many cases Boards and executive management are influenced by the views of those outside the organisation. Risk management is no exception and the following comment on the new ISO Risk Management Standard as well as Felix Kloman's views on the COSO document provide perspectives on the two current approaches on offer to Directors and CEO's as to how they should manage the risks confronting their organisations- the ISO 31000:2009 Standard along with its companion documents ISO/IEC 31010:2009 and ISO Guide 73 and the COSO Enterprise Risk Management framework.

The following paper outlines the content and spirit of the new Standard and has been printed in various publications leading up to and following the issue of ISO 31000.

AS/NZS ISO 31000:2009 – The New Standard For Risk Management

(Kevin W Knight AM)

Some would suggest that the Global Financial Crisis was caused by a failure of risk management rather than the failure of Boards and top management to effectively manage risk. The International Standards Organisation published *ISO 31000:2009 – Risk Management – Principles and guidelines* on 15th November 2009 and *ISO/IEC 31010:2009 – Risk Management – Risk assessment techniques* on 27th November 2009 to help industry and commerce, public and private to confidently emerge from the crisis.

Without risk there is no reward or progress, but unless risk is managed effectively within an organisation the opportunities will not be maximised and the threats minimised. Risk is all about uncertainty or more importantly the effect of uncertainty on the achievement of objectives. This is where ISO 31000:2009 is clearly different from existing guidelines on the management of risk in that the emphasis is shifted from something happening – the event – to the effect on objectives. Every organisation has objectives to achieve and in order to achieve those objectives it must manage any uncertainty that will have an effect on their achievement.

The Working Group that produced ISO 31000 brought together experts from some 28 countries representing all continents. All meetings of the Working Group had strong attendance numbers ranging from 40 to 60 delegates depending on the meeting location with a significant core group who participated in all meetings. It is precisely because of this core group, ably supported by the other expert delegates, and backed up by the national mirror committees that has ensured ISO 31000 represents the very best of contemporary thought on the management of risk and why the Australian & New Zealand Joint Technical Committee unanimously resolved to adopt it as AS/NZS ISO 31000:2009 and to consign AS/NZS 4360 to the history books.

ISO 31000:2009 sets out principles, a framework and a process for the management of risk that are applicable to any type of organisation. It does not mandate a one size fits all approach but rather emphasises the fact that the management of risk must be tailored to the specific needs and structure of the particular organisation.

Following a list of terms and definitions used in the document it sets out 11 principles that an organisation should address in order to assure it will effectively manage its risks and achieve its objectives. The principles need to be addressed by the Board and top management so as to ensure they are reflected in the policy of the organisation.

The next section looks at the framework that needs to be established to provide the foundations and arrangements that will embed the management of risk throughout the organisation at all levels. The framework section does not prescribe a management system to be adopted but rather emphasises the fact that the organisation should adapt the risk management components into its existing management system so as to ensure ownership of the policy and process by management and staff. The overarching component of the framework is the mandate and commitment of the Board and top management to the implementation, review and continual improvement of how risk is managed so as to ensure it is fully focused on the achievement of organisational objectives. This focus on the organisational objectives is imperative if Enterprise Risk Management (ERM) is to be achieved by way of a common language and process to manage risk throughout the organisation.

The framework calls for a clear understanding of the context in which the organisation operates so as to ensure the risk management policy clearly states the organisations commitment to the management of risk. Critically, the Standard requires that the organisation ensures there is accountability and authority for the management of risk by identifying risk owners as distinct from those who are responsible for implementing the decisions of the risk owner. The Standard seeks to differentiate between those who are "accountable" for managing risk (that is those persons with a liability, either corporate and/or legal, for their decisions or lack of decision) and those who are "responsible" for specific tasks (that is those persons with an obligation to carry out an instruction from a higher authority). The framework also sets out how the management of risk is to be woven into the organisational fabric so as to become an integral part of how things are managed within the organisation rather than having risk management as an add on or separate activity divorced from the mainstream line management of the business.
It is this enterprise wide approach to the management of risk that has caused a degree of dissent amongst the Working Group experts and national mirror committees. Many have maintained that safety and environmental matters should not be addressed under risk management as they are subjects that must be risk free. This viewpoint resulted in many

hours of discussion and debate within the Working Group which finally decided, by a very significant majority, that it was only through their inclusion in the risk management process that they would receive the attention by the Board and top management if they were to be effectively managed by the organisation.

The risk management process of communication & consultation; establishing the context; risk assessment consisting of the three steps of identification, analysis and evaluation; risk treatment; and monitoring & review follow the well worn path set by the Australian and New Zealand Standard AS/NZS 4360. The process set out needs to become an integral part of how the business is managed at all levels by being tailored to the business processes of the organisation so as to be woven into the culture and practices that make the organisation different from its competitors.

All activities should be traceable by way of records that provide the foundation for improvement in methods and tools, as well as in the overall process.

Finally an informative annex sets out the attributes of enhanced risk management for those organisations that have been working on managing their risks for some time and may wish to strive for a higher level of achievement.

ISO 31000 requires significant commitment of Board and top management attention as well as sufficient resources to make it a reality. It is not a tick and flick check list but a serious implementation of management activity to ensure it is enmeshed into the organisational fabric and culture across the organisation.

Many organisations prefer to spend time debating whether to introduce "total risk management" or "holistic risk management" or "enterprise risk management" or "enterprise wide risk management", or even "strategic risk management" others are content to settle for a tick and flick compliance programme that keeps the regulators happy. The successful organisations however work on identifying and understanding the risks involved in achieving their objectives and ensuring they manage them to a successful outcome.

Mr Kloman provided the following interesting and forthright comment from a North American perspective on the COSO approach to the management of risk:

COSO Enterprise Risk Management Framework 2004

Risk Management Reports Volume 31, Number 12.

The beast has at last produced its expected offspring, and a hulking, awkward creature it is. Given a gestation period of over three years, we might logically expect something that could immediately go forth and be useful but, alas, this creature is preceded by smaller, clearer-eyed and more nimble adversaries, leaving it to lumber away from its five parents (a biological marvel!) and gather dust when it finally settles to earth.

I speak, of course, of the long-awaited "final" version of the *Enterprise Risk Management – Integrated Framework*, produced by representatives of the five organizations that make up COSO, the Committee of Sponsoring Organizations of the Treadway Commission (American Accounting Association, American Institute of Certified Public Accountants, Financial Executives International, Institute of Management Accountants and the Institute of Internal Auditors). I reviewed its first draft in 2002, its second early in 2003 and its third late last year, after which I wrote about its weaknesses and strengths in the October 2003 *RMR.* While I acknowledge some improvement in this final effort, I'm afraid that its monstrous size and tedious prose (one appendix is made up entirely of passive sentences!) will condemn it to the dusty shelf, especially in comparison to the revised Australia/New Zealand Risk Management Standard 4360:2004. Consider that this COSO work is in two volumes totalling 230 pages, as compared to the lean and limber 28 pages of AS/NZS 4360. Yes, COSO's opening Executive Summary has been pared from 22 to 9 pages, meaning that several more senior executives and directors are likely to read it, but the excessive length of what's left has two significant deficits: too few will take the time to read it, and it dwells too heavily on an intricately detailed "process" that reeks of "controls." COSO slips into the fatal fallacy of trying to tell us "how" to do it, rather than "why." But because of the sheer volume of interest today in risk management, a partial result of Sarbanes-Oxley and similar initiatives around the world, COSO's version will receive broad distribution. It doesn't deserve it.

COSO continues to focus on risk as the potential for an *adverse* outcome. In an Appendix the authors acknowledge further discussion on this point but they conclude

"adding the concept of opportunity would cloud the concepts and make communication more difficult. Maintaining the distinction between a negative event and a positive one brings clarity to the enterprise risk management language." I continue to disagree, with respect, along with others in Australia, New Zealand, Canada, and UK and in ISO (whose glossary of 2002 comes down firmly on the idea that risk encompasses both positive and negative outcomes). An unexpected event may carry, simultaneously, potentially favourable and unfavourable results and recognizing them *together* creates the chance for a more intelligent organizational response.

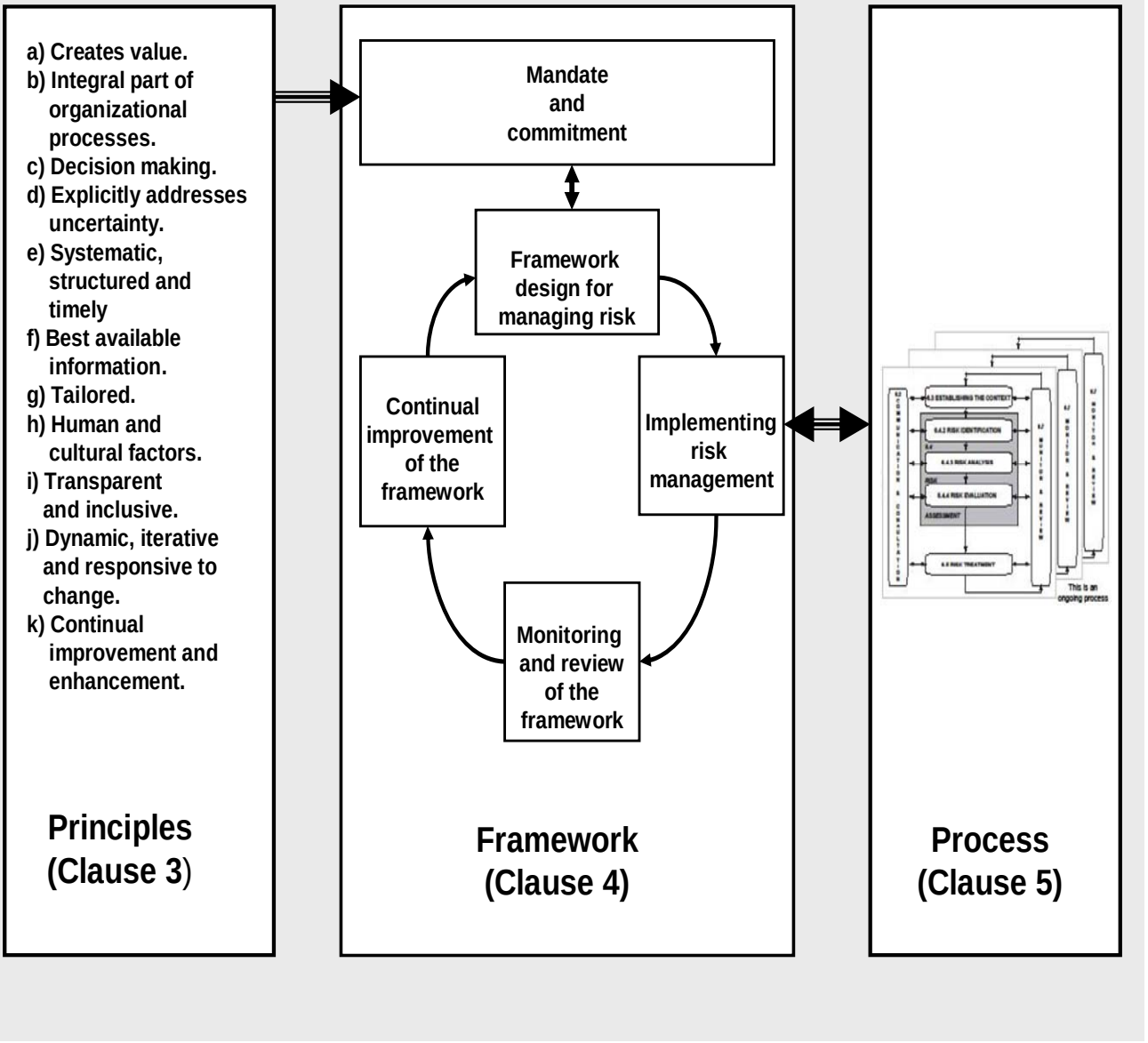
If we are trying to persuade others that enterprise risk management is a necessary alteration of organizational behaviour, why not adopt a definition that is brief and easily remembered? COSO weights us down with a 54 word slug: *"Enterprise risk management is a process, effected by an entity's board of directors, management and other personnel, applied in a strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives."* Compare that to AS/NZS 4360: *Risk management is the culture, processes and structures that are directed towards realizing potential opportunities whilst managing adverse effects."* Much better, but still not as memorable as my preference: "*risk management is a discipline for dealing with uncertainty."* Take your pick!

COSO's process remains at eight steps, compared to 4360's five. Again, if we want to communicate with others, why not reduce the process to two simple steps: *risk analysis* and *risk response*? I take no fault with the content of these other steps, but they can be included more effectively in later internal description and development. I do emphatically agree, however, with one COSO comment: "it is a multidirectional, iterative process in which almost any component can and does influence another." That's both the beauty and the challenge of learning to deal more intelligently with risk!

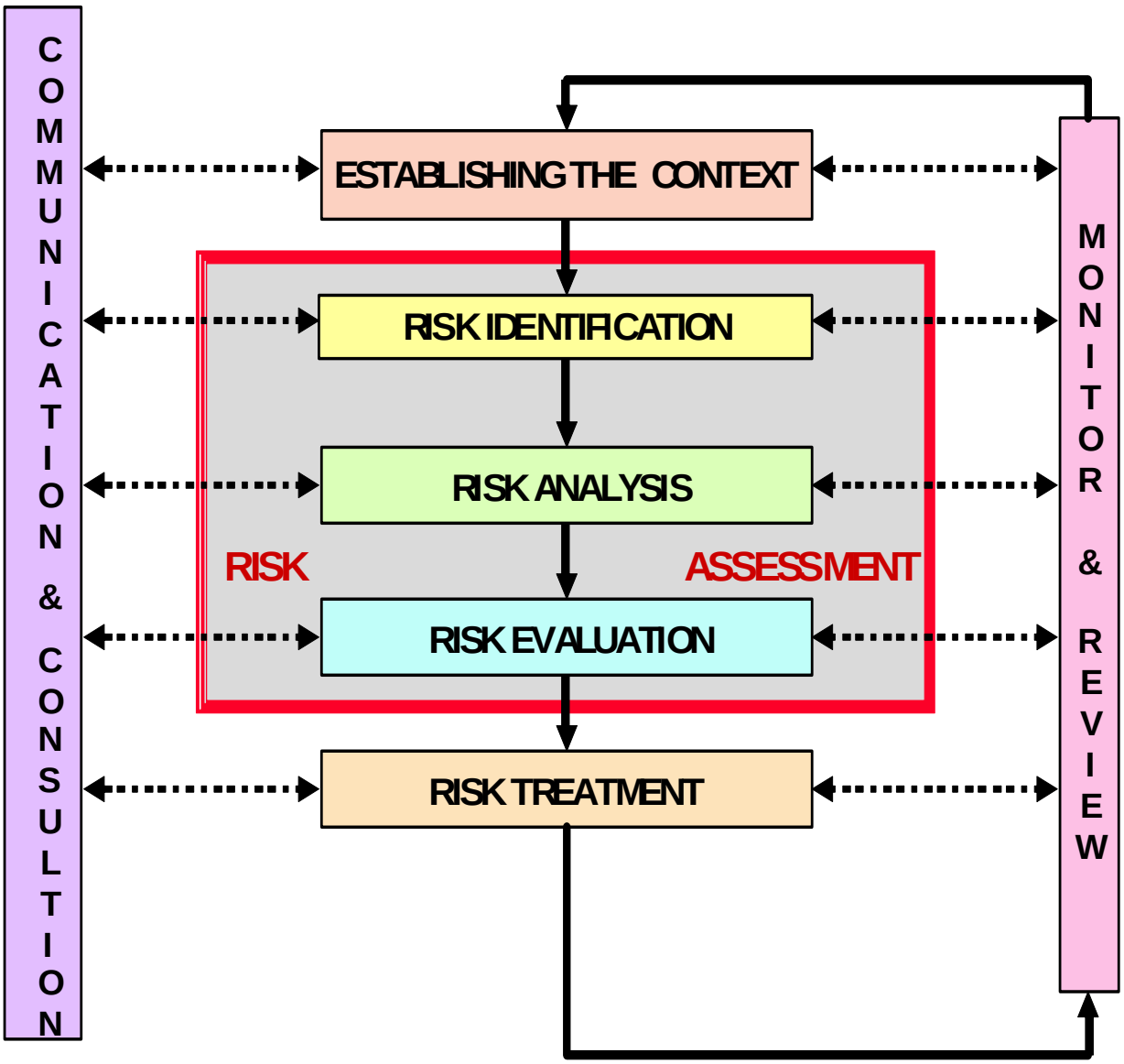
Despite my carping comments on length and prose, I do find much of value in COSO 2004. As a reference document I can recommend it be read and absorbed by students of the discipline. Let executives and directors read the Antipodean and UK versions!

Some quotations about the management of risk from executive managers, political leaders and decision makers in the Canadian Public Sector...

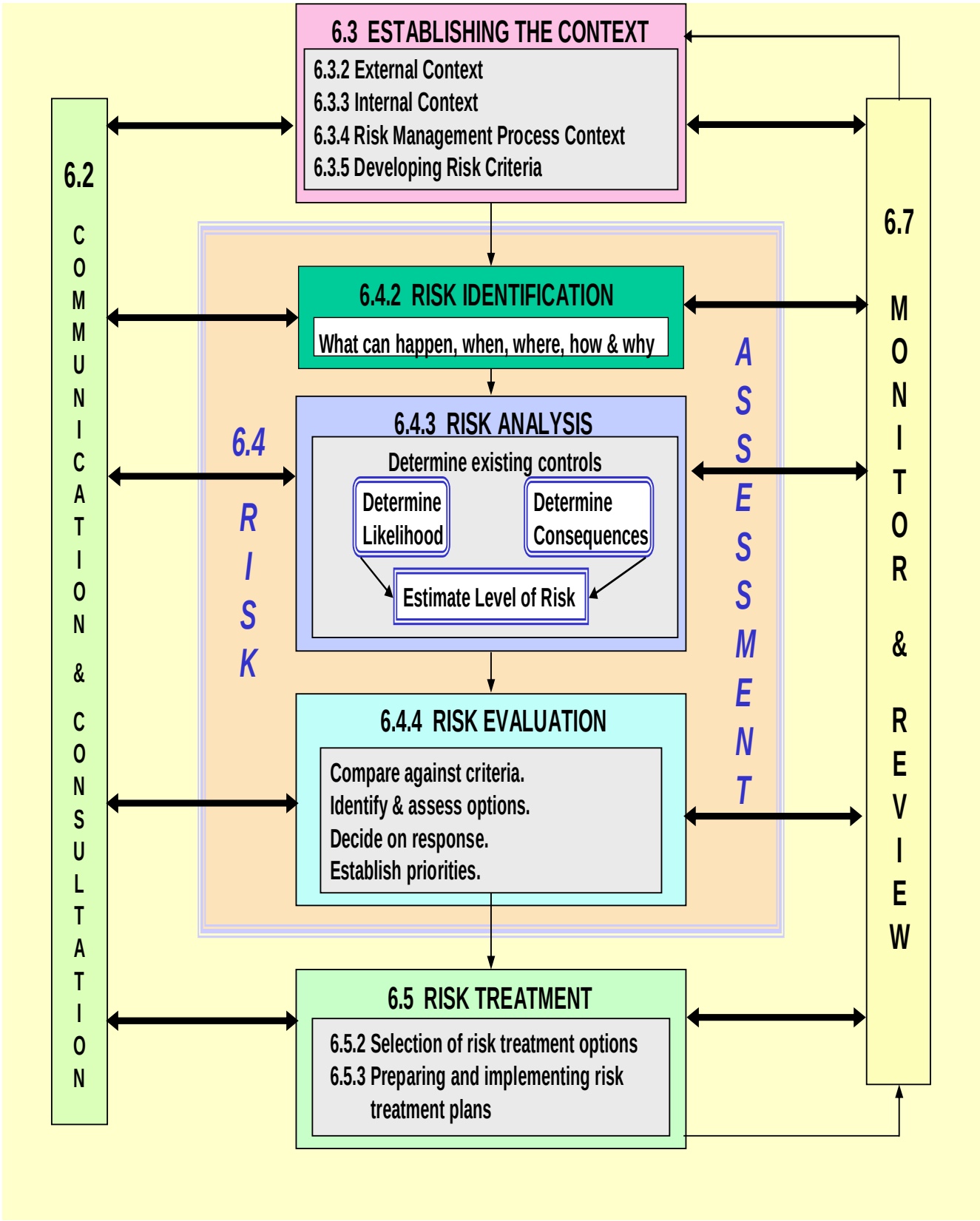
- *Due diligence is still a tick-the-box form-filling exercise. We have not embraced the substance of it.*
- ***We focus attention on the measurable, not the important**.*
- *We need to measure achievement in the context of a full team (governing body, management) not just one player - right now, we just don't do that.*
- ***Because we can't say things are 100% perfect, we resort to 'fuzzifying' it all.***
- *The government /legislature interface is dominated by a "shame & blame' mindset that is unlikely to change.*
- ***The vocabulary of public management has changed... almost everything we do is about risk management. Accepting that there is risk is part of the overall package.***
- *The major problem is not making mistakes but our apparent inability to learn from them.*
- ***If there is trust, performance information would be more meaningful.***
- *We pretend to report... they pretend to use it.* ***We (public servants) hide behind Ministers and they hide behind us.***



Relationship between the principles, framework and process in ISO 31000:2009

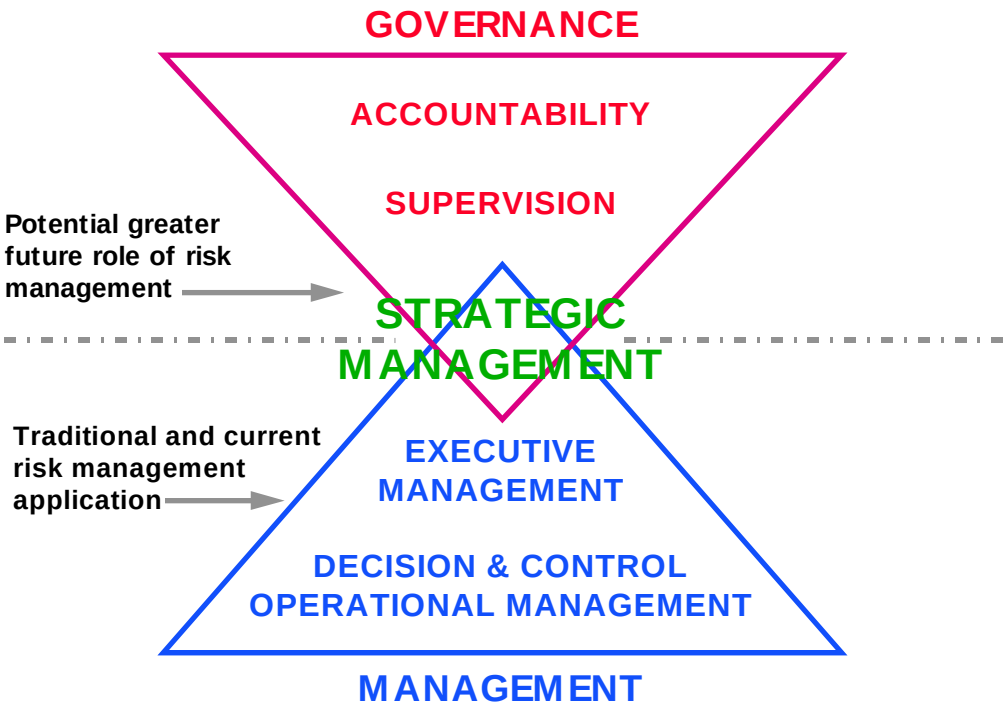


Overview of the ISO 31000:2009 Risk Management Process



Details of the ISO 31000:2009 Risk Management Process

The Risk Management Process within the Corporate Context



Boyd (1997) illustrates the relationship between management, risk management and corporate governance above. Corporate Governance activities are represented as four principal components: direction, executive action, supervision and accountability. The need for risk management to be undertaken at the strategic level of an organisation is highlighted.

This illustrates the current, and traditional, situation where risk management techniques are more highly evolved at the operational and tactical levels of an organisation.

Boyd, J., 1997, Risk Management's Role in Corporate Governance, Corporate Risk, Vol. 4, No. 8, August 1997

Basic Concepts

The Queensland Audit Office in November 2000 in a paper addressing governance made the following points.

Corporate governance is the way in which an organisation is controlled and governed in order to achieve its objectives. The control environment makes an organisation reliable in achieving these objectives within an acceptable degree of risk.

The key to understanding corporate governance is an understanding of the relationship between the organisation, objectives, risk management and control –

- An organisation is a group of people working together to achieve objectives. This definition is multilayered and may refer to the total organisation or any sub-groups thereof such as programs, business groups or project teams etc.

- Objectives are the goals an organisation sets for itself and similarly may be overall organisational objectives or more specific and related to sub-groups i.e. programs, business groups or project teams etc.

- Risk management is the process by which the impediments to an organisation achieving its objectives are professionally managed by identification, analysis, assessment, treatment and monitoring.

- The control environment is developed from the risk management process i.e. the identification and mitigation of the risks. Cost effective controls are equivalent to the treatment plans to manage risks.

- Strategies are the result offsetting objectives and risk management.

Corporate Governance Principles

The concept of corporate governance embodies a number of accepted management tools which have been around for some time. The value of corporate governance is that it draws these tools together into a logical, inter-related set of principles. To examine the inter-relationships it is necessary to revisit the definition of corporate governance.

> *Corporate governance is the way in which an organisation is governed and controlled in order to achieve its objectives. The control environment makes an organisation reliable in achieving these objectives within an acceptable degree of risk.*

- Inherent in this definition is the development of objectives and strategies through corporate planning and the establishment of controls to ensure that the objectives will be met.

- Operational plans are developed from the objectives and from these the organisational structure and the roles and responsibilities of members of the organisation are developed.

- Delegations are put in place to ensure that responsibility and accountability are matched with the necessary authority.

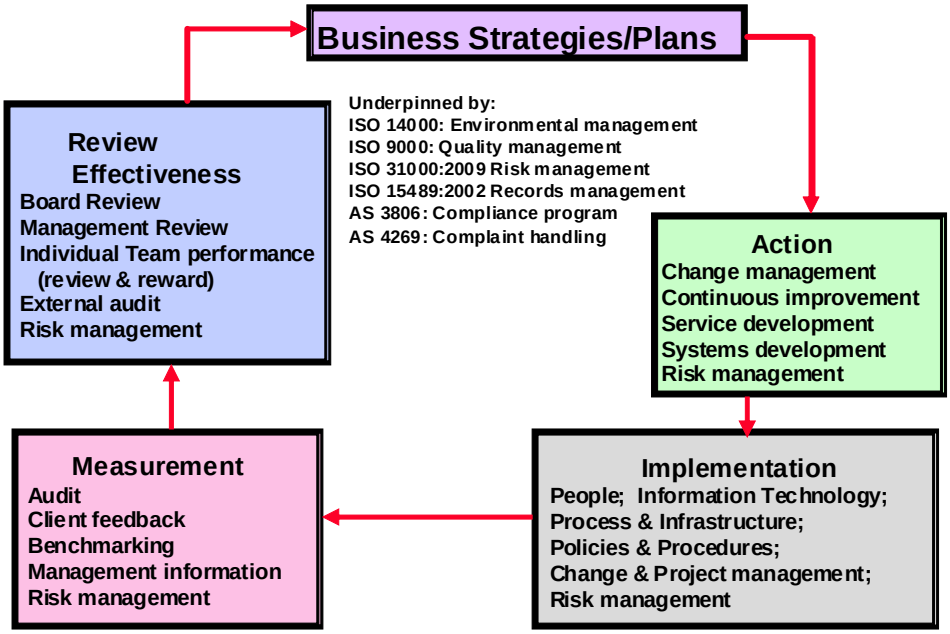
- A code of conduct provides members of the organisation with the expected standard of behaviour and is directed at fraud prevention, client service and creating a culture which favours continuous improvement.

- Reporting and monitoring processes are developed to ensure
    - conformance with laws, policies, procedures, and the code of conduct
    - performance against the corporate and operational plans.

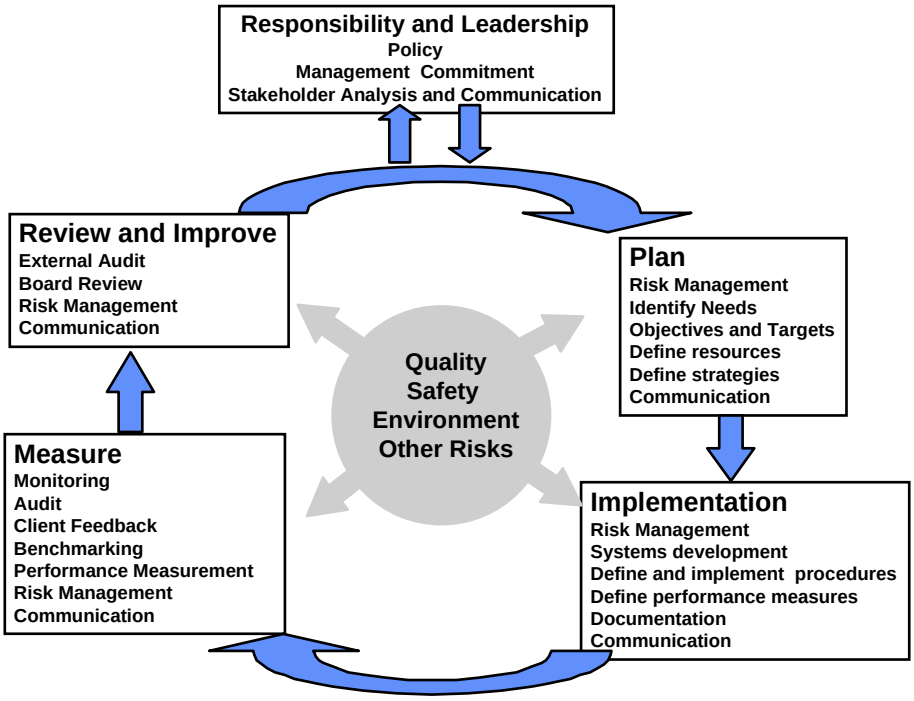
- Internal and external reporting provides accountability.

Corporate governance may be regarded as the glue which holds an organisation together in pursuit of its objectives. Risk management provides the resilience.

An Integrated Management System to Ensure Progress in Strategy Implementation



Develop and implement an infrastructure or arrangements to ensure that management of risk becomes an integral part of the planning and management processes and general culture of the organisation.



Risk Management Committee Models

Focused, integrated plan that provides clear goals, success measures and critical path that can be explained to all stakeholders

- Develop a three year plan with annual budget that focus on a small number of key risk reduction programs that touch broadly across the Business and address key issues of risk that significantly impact the Business
- Culture changing approach
- Reflects the Ways of Working
- Allows an opportunity to broaden the "cut" once the program bites.

Stakeholder Identification

ISO 31000:2009	**5.2** ..... Communication and consultation with stakeholders is important as they make judgements about risk based on their perceptions of risk. These perceptions can vary due to differences in values, needs, assumptions, concepts and concerns of stakeholders. As their views can have a significant impact on the decisions made, the stakeholders' perceptions should be identified, recorded, and taken into account in the decision making process. Communication and consultation should facilitate truthful, relevant, accurate and understandable exchanges of information, taking into account confidential and personal integrity aspects.

At the earliest opportunity, it is essential to identify the stakeholders in a proposed risk management study. Stakeholders can include:

- customers;
- decision-makers;
- individuals inside the organisation, such as employees, management,
- individuals or groups who are interested in issues related to the proposal.
- individuals who are, or perceive themselves to be, directly affected by a decision or activity;
- non-government organisations such as environment groups and public interest groups;
- partners in the decision, such as financial institutions and insurance agencies;
- politicians (at all levels of government) who may have an electoral or portfolio interest;
- regulators and other government organisations that have authority over activities; senior management, contractors, and volunteers;
- suppliers and service providers;
- the media, who are likely stakeholders as well as conduits of information to other stakeholders; and
- union and/or staff representative groups;

Throughout the study, the mix of stakeholders may change. New stakeholders may join and wish to be included in any considerations, while others may drop out, through no longer being involved in the process. (e.g. when the decision has been taken to avoid an activity.) Consequently, the stakeholder consultation process should be continuous and, as such, should be included as an integral part of the risk management process.

Note that the level of stakeholder concern may change in response to new information, either because the stakeholder's needs and concerns have been addressed, or because new information has given rise to new needs, issues and/or concerns. Note also that it is valid for different stakeholders to have different opinions and different levels of knowledge regarding a particular issue. Care must be taken to balance these legitimate interests while avoiding involvement of those who would use the process as a forum for other purposes.

The purpose of a stakeholder analysis is to provide decision-makers with a documented profile of stakeholders so as to better understand their needs, issues and/or concerns. The stakeholder analysis also provides the basis for the development of messages that decision-makers may wish to deliver to other stakeholders as part of the communication and consultation process. Note that information captured through stakeholder analysis may or may not be shared with other stakeholders, depending on such issues as the uncertainty of the information at the time and/or the need to keep certain information confidential for the time being.

An important stakeholder can be a non-governmental organisation (NGO) which is an organisation independent of government, in the sense that it is not created by law – it comes into existence on the initiative of non-governmental actors. The term generally refers to lobby or advocacy groups, whose aim is it to influence government policy making and/or implementation. NGOs come in a

variety of shapes and sizes. They range from small community action groups campaigning against the building of mobile phone masts, to national trades unions and chambers of commerce who seek to represent the interests of their members, through to larger multinational campaign groups such as Greenpeace and Amnesty International.

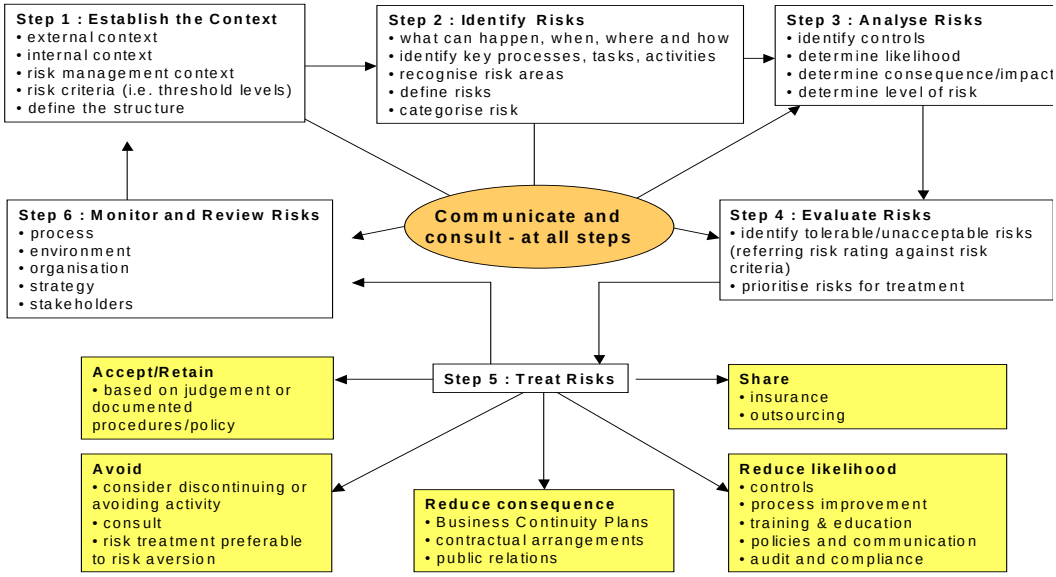
Understanding stakeholders will assist in the development of marketing and communication strategies

Communicate and Consult

> An effective risk communication policy includes commitments to: open and honest communication; early release of information; meaningful processes for explaining risks; processes for incorporating community concerns and values; shared decision-making; and a relationship built on trust.
>
> **Jean Mulligan, Elaine McCoy and Angela Griffiths, *Principles of Communicating Risks,***
> **The Macleod Institute for Environmental Analysis, University of Calgary, Calgary, Alberta 1998**

It is important to communicate and consult with stakeholders at each step in the risk management process. This is illustrated below**.**

Risk communication and consultation can be defined as any two-way dialogue between stakeholders about the existence, nature, form, severity, or acceptability of risks.



Communication & Consultation

At the earliest stages in the risk management process, it is important to develop a risk communication strategy. Communication efforts must be focussed on consultation, rather than a one-way flow of information from decision-makers to stakeholders, especially those outside the immediate organisation. To initiate the consultative process, those responsible for developing the risk management proposal should identify key stakeholders and where practicable institute a communication programme.

Consultation between experts and laypersons can be difficult for a number of reasons. Experts and laypersons will often have vastly different levels of knowledge related to specific issues. There are often large uncertainties associated with estimating future likelihood's or consequences, and concerns that technical experts may overlook or fail to acknowledge legitimate community fears. When technical experts disagree amongst themselves, they decrease the acceptability of the analysis in the eyes of the layperson.

Consequently, communication and consultation are critical to ensure that stakeholders have access to relevant information. It is also critical that this information be presented in a manner that the recipients understand.

Perceptions of Risk

Perceptions of risk can vary significantly between technical experts, project team members, decision-makers and stakeholders. For this reason, the need to effectively communicate the level of risk involved in a treatment plan is essential if an informed, valid decision is to be made.

Stakeholder perception of risks may vary due to differences in assumptions, conceptions, and the needs, issues or concerns as they relate to the risk or issue under discussion. Stakeholders are likely therefore to make judgements of the acceptability of a risk based on their perception of the risk. Since stakeholders have the most impact on the decision-making process, it is important that their perceptions of risks, as well as their perceptions of benefits, be identified, documented and the underlying reasons for them understood.

Thus people's perceptions of the risks are informed by a number of factors that may not seem relevant to experts making technical assessments of the same risks and individuals and communities respond to risk and risk information according to their perceptions and understanding of the risk, though the links may at time be complex.

Perceptions of risk can vary significantly between technical experts, project team members, decision-makers and stakeholders. When people perceive risk differently they will react differently, and this needs to be taken into account when developing risk treatments where individual responses will affect their viability.

Technical experts tend to emphasise factors in terms of the probability of an occurrence or its likelihood and consequences, while a lay-person tends to emphasise factors such as: -

- whether the risk is voluntary or involuntary, and the (perceived) measure of control over the risk
- whether the risk is familiar or unfamiliar
- whether the risk is `new'
- whether the consequences are likely to be common or dread; immediate or delayed; chronic, cumulative or catastrophic in nature
- the severity of the consequences

Other factors include: -

- the degree of personal exposure and the necessity of exposure
- the size of the group exposed
- the effect on future generations;
- the global catastrophic nature of the risk
- the changing character of the risk
- whether there is seen to be any easy way of reducing the risk and the availability of alternatives
- whether the hazard is encountered occupationally
- whether there is likely to be misuse
- whether the consequences are reversible
- whether there is a desirable element such as an opportunity to the consequences (need to balance reward with risk)

Different factors take precedence for different types of risk, or risks of similar character encountered under different circumstances. In addition to these factors, or hazard characteristics

a number of demographic and socio-economic determinants such as age, sex, education, social class and income strata will affect individual and group perceptions.
Perceptions of risk may vary due to differences in assumptions, conceptions, and the needs, issues and/or concerns as they relate to the risk or issue under discussion. Stakeholders are likely therefore to make judgements of the acceptability of a risk based on their perception of the risk. Since stakeholders have a large impact on the decision-making process, it is important that their perceptions of risks, as well as their perceptions of benefits, be identified, documented and the underlying reasons for them understood.

Outrage is a term that has been used to describe the reaction of the public to certain risks that they believe are being imposed on them. It is convenient 'shorthand', and comprises a subset of the hazard factors listed above. The factors that trigger 'outrage' are related to the degree of 'voluntariness', familiarity, control, equity, and moral relevance, whether the risk is 'dread' and distribution in time and space.

Risk managers should consider these factors carefully in cases where community reaction to activities may have an impact.

> Communicating risk successfully is neither a public relations nor a crisis communications exercise. Its aim is not to avoid all conflict or to diffuse all concerns. Risk communication seeks to improve performance based on informed, mutual decisions with respect to … risk.
>
> **Jean Mulligan, Elaine McCoy and Angela Griffiths, *Principles of Communicating Risks,***
> **The Macleod Institute for Environmental Analysis, University of Calgary, Calgary, Alberta 1998**

Establishing the context

ISO 31000:2009	**5.3 ESTABLISHING THE CONTEXT** **5.3.1 General** By establishing the context, the organization articulates its objectives and defines the external and internal parameters to be taken into account when managing risk, and sets the scope and risk criteria for the remaining process. While many of these parameters are similar to those considered in the design of the risk management framework (see 4.3.1), when establishing the context for the risk management process, they need to be considered in greater detail and particularly how they relate to the scope of the particular risk management process. **5.3.2 Establishing the external context** …. Understanding the external context is important in order to ensure that the objectives and concerns of external stakeholders are considered when developing risk criteria. It is based on the organization-wide context, but with specific details of legal and regulatory requirements, stakeholder perceptions and other aspects of risks specific to the scope of the risk management process…. **5.3.3 Establishing the internal context** …. The risk management process should be aligned with the organization's culture, processes, structure and strategy. Internal context is anything within the organization that can influence the way in which an organization will manage risk …. **5.3.4 Establishing the context of the risk management process** The objectives, strategies, scope and parameters of the activities of the organization, or those parts of the organization where the risk management process is being applied, should be established. The management of risk should be undertaken with full consideration of the need to justify the resources used in carrying out risk management. The resources required, responsibilities and authorities, and the records to be kept should also be specified…. **5.3.5 Defining risk criteria** The organization should define criteria to be used to evaluate the significance of risk. The criteria should reflect the organization's values, objectives and resources. Some criteria can be imposed by, or derived from, legal and regulatory requirements and other requirements to which the organization subscribes….

At the outset clearly define the goals that need to be accomplished. What are the performance measures that will indicate achievement of these aims?

Since the management of risk is done at various levels, the final goal might be high-level strategic outcomes and program outputs. It may be the reason an activity or project is undertaken. In procurement work, the objective may be to obtain value for money or assist in regional development. In providing grants, it may be to address a defined socio economic need.

Identifying the business objective and related performance measures is the first step before going on to determine what risks need to be managed in order to achieve these goals. Thus the risk management process provides an opportunity to consult with others and clarify business directions.

The legislative, political, cultural and socio-economic environment must be taken into account when managing risk.

Managers at all levels should review their role in contributing to the wider Organisational strategies and objectives when making decisions about risk. Think about risk in the broader organisational context – what are the strategic and operational objectives how are they to be achieved. Who are the stakeholders? What is their perception of risk? What management priorities will be factored into specific risk analysis and action planning?

The management of risk may be part of a broader planning process, for example an annual business plan or project plan. If so, risk context can be considered as part of the broader planning process. Environmental scanning and specification of the business objectives in a business plan can feed into the risk management process.

If the risk assessment is for a particular project it is advisable to analyse the project plan, particularly the assumptions which underpin the project. If the assessment is directed towards a community or organisation it is essential to understand the relationships and the people involved.

Identify risks

ISO 31000:2009	**5.4.2 RISK IDENTIFICATION** The aim of this step is to generate a comprehensive list of risks based on those events that might create, enhance, prevent, degrade, accelerate or delay the achievement of objectives. It is important to identify the risks associated with not pursuing an opportunity. Comprehensive identification is critical, because a risk that is not identified at this stage will not be included in further analysis.

This step requires identification of risks which arise from all aspects of the environment identified in the previous step. Unidentified risks can pose a major threat to the organisation. It is important to ensure that the widest range of risks are identified.

Risk identification involves examining all sources of risk and the perspective of all stakeholders, both internal and external. It is important to identify each source so that the analysis can consider the contribution each makes to the likelihood and the consequences of the risk. A risk assessment may concentrate on one or many possible areas of impact relevant to the organisation or activity, but a standard methodology should be applied across all functions.

Valid information is important in identifying risks and in understanding the likelihood and the consequences of the risk. Although it is not always possible to have the best, or all information, it should be as relevant, comprehensive, accurate and timely as resources will permit.

Existing information sources need to be accessed and, where necessary, new data sources developed. Some risks will not lend themselves to objective analysis or observation, and the cost of collecting all data might be too great for the benefits provided.

It is essential that staff undertaking this step are knowledgeable about the policy, program, process, or activity being reviewed. Where it is complex, there may be very few people who understand all of its elements and it may be best to work with a group.

Components of a risk

A risk is associated with:

(a) A **source** of risk or hazard.

(b) An **event or incident** – something that occurs such that the source of risk has the impact concerned.

(c) A **consequence**, outcome or impact on a range of stakeholders and assets.

(d) A **cause** (what and why) (usually a string of direct and underlying causes) for the presence of the hazard or the event occurring.

(e) **Controls** and their level of effectiveness.

(f) **When** could the risk occur and **where** could it occur.

These components of risk should not be confused and need to be separately identified. Ideally, a risk should be identified in the following terms:

(Something happens) leading to (outcomes expressed in terms of impact on objectives).

For example:

- A thunderstorm damages goods leading to cost of rework.
- We identify a market niche leading to increased sales.
- A spill of oil in the creek damages our reputation with the local community.

Possible methods of identifying risks

audits or physical inspections;
brainstorming;
decision trees;
examination of local or overseas experience;
expert judgement;
flow charting, system design review, systems analysis, systems engineering techniques;
interview/focus group discussion;
operational modelling;
personal experience or past organisational experience;
scenario analysis;
strengths, weaknesses, opportunities and threats (SWOT) analysis;
survey, questionnaire; and
work breakdown structure analysis.

Possible sources of risk

business interruption;
commercial/legal relationships;
custody of information including the duty to provide and to withhold access;
financial/market;
management activities and controls;
natural events;
occupational health and safety;
personnel/human behaviour;
political/legal;
property/assets;
public/professional/product liability;
security;
socio-economic;
technology/technical; and
the activity itself/operational.

Possible areas of risk effect

asset and resource base cost: both direct and indirect;
community;
intangibles;
natural environment;
organisational behaviour;
people;
performance of activities: how well the activity is performed; and
timeliness of activities: including start time, downstream or follow-up impacts.

Checklist of the types of exposures managers may have to manage

The purpose of this list is to provide a list of potential exposures that managers might face. The list is not exhaustive, but it should give managers an indication of exposures which may affect their business and therefore have to be managed.

HUMAN RESOURCE MANAGEMENT

- Enterprise Bargaining disputes
- over-reliance on a small number of staff
- problems with outside contractors
- problems with own staff
  - badly designed workplaces
  - claims of sexual harassment
  - criminal activity
  - cultural/religious conflicts
  - Equal Employment Opportunity/Anti-Discrimination disputes/litigation
  - inadequate/inappropriate training
  - inappropriate skills mixes
  - industrial disputes
  - insufficient technical skills
  - language difficulties
  - loss of key staff
  - Occupational Health and Safety disputes
  - unfair dismissals/litigation

PERSONNEL

- loss of key personnel
- poor industrial relations
- skills, training
- succession planning
- theft, misappropriation
- wrongful acts

OPERATIONAL

- badly designed product
- breaches of *Trade Practices and Fair Trading Acts*
- contaminated or unsafe products
- contaminated raw materials
- equipment
  - breakdown
  - unavailability of parts
- inexperienced personnel
- planning and scheduling conflicts
- poor service leading to angry customers
- poorly maintained equipment and/or infrastructure
- superseded equipment
- supply delays

FINANCIAL

- asset/liability management
- audit risk
- bad debts
- cash/fund management shortfall

FINANCIAL (Cont.)

- business interruption
  - industrial action
  - interruption of supply
  - loss of records
  - machine breakdown
  - utilities interruption
- exchange rate movements
- fines/judgement orders
- fraud
-
- inaccurate accounting and/or reporting systems
- inadequate costing systems (leading to unsustainable pricing)
- inadequate insurance
- inventory risk
  - obsolescence
  - stock losses
- negligence
- poor cashflow
- over-reliance on a small number of customers/suppliers

DISASTERS WHICH AFFECT SENIOR AND KEY STAFF

- accidents (eg. vehicle, aeroplane, train)
- key individual losses

NATURAL AND MAN-MADE DISASTER

- arson
- attack by deranged persons
- community exposure to pollution
- electrical 'spikes'
- epidemic among staff
- espionage
- fire
- flooding
- industrial accidents
- lightning strikes
- power cuts
- sabotage
- malicious damage/vandalism/terrorism
- staff exposure to long-term hazards and pollution
- water cuts

POLITICAL

- changes in Government
- community expectations
- legislative changes

TECHNOLOGICAL CHANGE

- materials may be supplanted
  - aluminium in warships replaced by high-grade steel
  - ceramics may supplant steel in car engines

TECHNOLOGICAL CHANGE (Cont.)

- fibreglass and aluminium supplanted wood in small boats
- processes may be made obsolete
  - computer-aided manufacture supplanted conventional manufacturing
- whole industry might be wiped out
  - artificially-produced wine may replace conventional wine
- competitors may innovate successfully
- exogenous
  - change in tariffs or levels of protection
  - cheap PCs make word-processors and typewriters almost obsolete
  - synthetics affected wool and other natural fibres
  - the oil shock of 1973 increased demand for small, fuel-efficient cars

ECONOMIC CYCLE/MARKETING

- defective/dangerous products
- import competition
- limited range of products
  - broaden product range, include some products which are counter-cyclical
- loss of distribution rights or marketing channels
- undetected changes in market/customer demands

CONTRACTUAL/ LEGAL

- breach of contract
- directors and officers liability
- errors and omissions
- limitation of liability
- product liability
- public liability
- statutory breaches

BUSINESS ACTIVITY BY-PRODUCTS

- client service
- computer breakdown
- contingency planning/business resumption
- occupational injury, illness, physical security, property loss

Key questions in identifying risks

What are the accountability mechanisms - internal and external?
What are the consequences of each risk?
What are the stakeholders' expectations of the organisations performance?
What controls presently exist to mitigate this risk?
What is the need for research into specific risks?
What is the potential cost of each risk?
What is the reliability of the information?
What is the scope of this research?
What is the source of each risk?

What resources are needed to carry out the research?
When, where, why, how are the risks likely to occur, and who might be involved?

Documentation of this step

For a small process this step may be documented by a simple tabulation.
More complex documentation may be required for a larger process.
List each risk; identify its source and consequences.
Classify risks under functional groups if appropriate.
Identify each control process.
Identify areas of research if appropriate.

Analyse risk

ISO 31000:2009	**5.4.3 Risk analysis** Risk analysis involves developing an understanding of the risk. Risk analysis provides an input to risk evaluation and to decisions on whether risks need to be treated, and on the most appropriate risk treatment strategies and methods. Risk analysis can also provide an input into making decisions where choices must be made and the options involve different types and levels of risk….

The level of risk is defined by the relationship between consequence and likelihood applicable to the area of risk or program under review.

Qualitative analysis may be used where the level of risk does not justify the time and resources needed to do a numerical analysis, where the numerical data are inadequate for a more quantitative analysis, or to perform an initial screening of risks prior to further, more detailed analysis.

The value of qualitative analysis is enhanced when the determination of risk is shared across a range of people with varying backgrounds and interests. One person's view may be different from another's and the contribution of many ideas may improve the usefulness of the outcome.

A semi-quantitative approach allocates numbers to qualitative word ranking's such as high, medium and low, or to more detailed descriptions for likelihood and consequence. These rankings are shown against an appropriate numerical scale for calculating the level of risk. Information can then be processed for analysis using arithmetic methods.

If using a semi-quantitative approach, it is important not to interpret the results to a finer level of precision than is actually contained in the initial word rankings. Do not use the numbers to give an appearance of precision where it does not exist.

The level of risk can be calculated using a quantitative method in situations where the likelihood of occurrence and the consequences can be quantified. For example, fraud risk assessments tend to be quantitative. This method is particularly valuable in providing a ranking of residual risks to identify a prioritised list of action areas.

In many instances relatively straightforward methods are used effectively, although some of the case studies indicate the use of more refined techniques, or the intention to pursue these refined techniques in the future.

However, even sophisticated quantitative techniques may have their weaknesses and these need to be kept in mind. **(See ISO/IEC 31010:2009)**.

An example of tables to determine the level of risk from the likelihood and consequences are shown on the next pages.

Note: The descriptors utilised in these examples are used with respect to the organisation rather than the individual hence the use of Extreme in lieu of Catastrophic for the highest consequence, and have been chosen to avoid duplication in any matrix or subsequent report.

Likelihood

Likelihood Example

Descriptor	Description	Indicative Frequency
Almost certain	The event will occur in most circumstances	Once a year or more frequently
Likely	The event will probably occur at least once	Once every three years
Possible	The event might occur at some time	Once every ten years
Unlikely	The event is not expected to occur	Once every thirty years

Another approach to likelihood scales is this one (contained at clause 2.4.28 of *ACSI 33*) which uses a five-level approach to rating likelihood.

If a risk…	Then an appropriate likelihood rating is…
is expected to occur in most circumstances,	almost certain.
will probably occur in most circumstances,	likely.
might occur at some time and may be difficult to control due to some external influences,	possible.
could occur some time,	unlikely.
may occur only in exceptional circumstances,	rare.

Source: Australian Department of Defence 2005, p. 2-32.

Yet another likelihood scale, which also uses a five-level approach to rating likelihood.

Rating	Description
Almost certain	Significant past history, and considered most likely in these circumstances
Likely	Some past history, and considered quite likely in these circumstances
Possible	Some past history, and considered possible in these circumstances
Unlikely	No past history, but possible in some circumstances or occasionally
Rare	No past history, and considered unlikely to occur

In deciding on the likelihood scale to use one must take into account not only the history of past events, but also allow the aspects of knowledge, resources and motivation of the relevant threat sources to be taken into account.

It is important to note that there is no approach that is ‘right’ or ‘wrong’ for assessing the likelihood; each organisation needs to develop a set of ‘likelihood ratings’ that are appropriate for use in assessing the different types of risk relevant to that organisation.

Consequences

Consequence Example focusing on a variety of organisational impacts of risk.

Consequence Category (in order of severity) ▸▸ / **Factor of Consequences** (in alphabetical order) ▾▾	**MINOR**	**MAJOR**	**EXTREME**	**CRITICAL**
Disruption to established routines/ operational delivery.	Some disruption manageable by altered operational routine.	Disruption to a number of operational areas within a location or region & possible flow on to other locations/ regions.	All operational areas of a location or region compromised. Other locations /regions may be affected.	Total system dysfunction. Total shut-down of operations.
General environmental & social impacts.	Short term, local detrimental effect on the environment or social impact, eg. significant discharge of pollutants within local neighbourhood.	Serious, local discharge of pollutant or source of community annoyance within general neighbourhood that requires remedial action.	Long term detrimental environmental or social impact i.e., chronic &/or significant discharge of pollutant.	Extensive detrimental long term impacts on the environment and community i.e., catastrophic &/or extensive discharge of persistent hazardous pollutant.
Financial. (Organisation as a whole or of any single unit**).**	-2 % of monthly budget &/or $40000 limit.	-5 % of monthly budget &/or $ 100000 limit.	-10% of monthly budget &/or $500000 limit.	-15% of monthly budget &/or $1000000 limit.
Management **Corporate.**	Staff & management dissatisfaction - broader basis.	CEO's dissatisfaction Likelihood of legal action.	CEO & Board dissatisfaction. Legal action.	General Manager's /Regional Manager's and/or CEO's resignation/ removal.
Operational.	Dissatisfaction disrupts production.	Significant disruption to operations.	Qualified Audit report to Board naming particular managers.	Location management resignation/ removal.
Damage to Reputation.	Significant adverse publicity in particular locations.	Significant adverse publicity State-wide.	Sustained adverse publicity State-wide. Chairman of Board dissatisfaction.	CEO &/or Chairman of Board resignation/ removal.
Security.	Localised Incident. No effect on operations.	Localised incident. Significant effect on operations.	Significant incident effecting multiple locations.	Extreme incident effecting organisations survival.
Workplace Health & Safety.	Injury – no lost time.	Injury – lost time Compensatable Injury.	Serious injury/stress resulting in hospitalisation.	Multiple Fatality (not natural causes)..

Table to determine the level of risk

The following table illustrates the descriptors that may be used combining the example of likelihood and the example of consequences.

	Consequences			
Likelihood	**Minor**	**Major**	**Extreme**	**Critical**
Almost Certain	Medium	High	Serious	Serious
Likely	Low	Medium	High	Serious
Possible	Low	Medium	High	High
Unlikely	Low	Low	Medium	High

Legend:

- **Serious risk;** immediate action required, senior management/Board will be accountable
- **High risk;** senior executive management attention needed and management accountability and responsibility specified
- **Medium risk;** manage by specific monitoring or response procedures by accountable Line managers
- **Low risk;** manage by routine procedures, unlikely to need specific application of resources.

The 'risk matrix' below is based on clause 2.4.32 of *ACSI 33*. It uses five ratings for both 'likelihood' and 'consequences', and results in four levels of assessed risk: Extreme, High, Moderate and Low.

	Consequences				
Likelihood	***Catastrophic***	***Major***	***Moderate***	***Minor***	***Insignificant***
Almost certain	E	E	E	H	H
Likely	E	E	H	H	M
Possible	E	E	H	M	L
Unlikely	E	H	M	L	L
Rare	H	H	M	L	L

Legend:

E = Extreme (requires detailed research and management planning at an executive level)

H = High (requires senior management attention)

M = Moderate (can be managed by specific monitoring or response procedures)

L = Low (can be managed through routine procedures).

Source: Australian Department of Defence 2005, p. 2-32.

The table below (which is similar to Table 6.7 in Standard Australia's *HB 436:2004* (p. 56) is an example of a simple risk matrix, with a different 'risk treatment key'.

	Consequences		
Likelihood	***VeryHigh***	***Medium***	***Very Low***
Highly Likely	Priority 1	Priority 1	Priority 2
Possible	Priority 1	Priority 2	Priority 3
Rare	Priority 2	Priority 3	Priority 3

where:

Priority 1 = Urgent action required immediately.

Priority 2 = Targeted action needed.

Priority 3 = To be managed through standard operating procedures.

Recognising and Exploiting Opportunities

Many risk analyses are directed to the negative consequences of risks, and the consequence scales reflect the losses or undesired outcomes that might arise. However, the risk management process can be used to identify and prioritise opportunities (or 'positive' risks) with little change to the process.

When considering opportunities, the likelihood scale need not change, as this reflects the chance that a beneficial outcome will arise, but the consequence scale must be adjusted. This can be done in two ways.

- The simplest approach, when opportunities are being considered by themselves (without negative impacts), is to use a consequence scale similar to that for risk analysis, but with only positive outcomes. An example is shown in the table below. The measures used should reflect the needs and nature of the organisation and activity under study.

Level	Descriptor	Example of Detailed Description for Positive Consequences
1	Insignificant	Small benefit, low financial gain
2	Minor	Minor improvement to image, some financial gain
3	Major	Some enhancement to reputation, high financial gain
4	Outstanding	Enhanced reputation, major financial gain
5	Extreme	Significantly enhanced reputation, huge financial gain

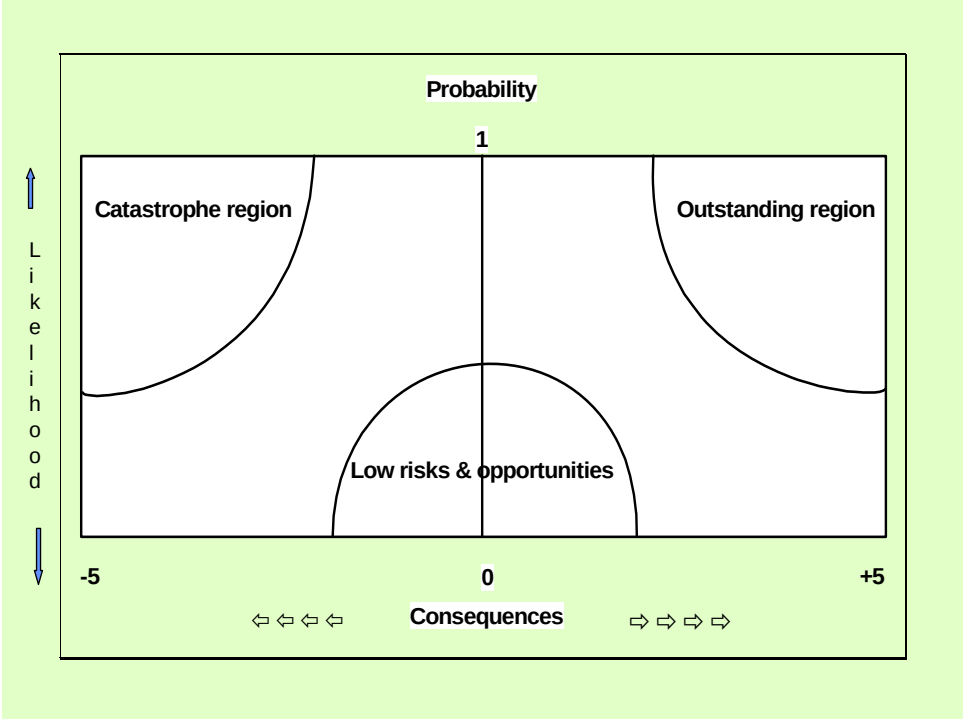
A qualitative opportunity analysis matrix can be used to determine the level of opportunity. All that need change is the legend, with the focus of action being on capturing and exploiting the opportunity rather than avoiding or mitigating the problems.

S = superior opportunity; detailed planning required at senior levels to prepare for and capture the opportunity
H = high opportunity; senior management attention needed
M = moderate opportunity; management responsibility must be specified
L = low opportunity; manage by routine procedures

- When risks and opportunities are being considered together, a 'two-directional' scale of consequences may be appropriate, with – 5 representing a catastrophic risk and + 5 representing an outstanding opportunity. The analysis matrix must be adjusted too. The matrix below shows an example to explore**.**

-S	-S	-S	-S	**A Almost certain**	H	S	S	S
-S	-S	-H	-H	**B Likely**	H	H	S	S
-S	-S	-H	-M	**C Possible**	M	H	S	S
-S	-H	-M	-L	**D Unlikely**	L	M	S	H
-H	-H	-M	-L	**E Rare**	L	M	H	H
-5	-4	-3	-2	⇑ **Likelihood**	+2	+3	+4	+5
Extreme	**Critical**	**Major**	**Minor**		**Minor**	**Major**	**Outstanding**	**Extreme**
Negative consequences					**Positive consequences**			

If semi-quantitative or quantitative scales are used, individual risks and opportunities can be plotted on the same graph to show their relative levels. The diagram shows an example in which the horizontal consequence scale ranges from – 5 (catastrophic negative outcome) to + 5 (outstanding beneficial outcome), and the likelihood's are shown on a vertical probability scale from 0 to 1.



Key questions in analysing risk

How confident are you in your judgement?
What are the current controls which may - prevent, detect or lower the consequences of potential or undesirable risks/events?
What are the potential consequences of the risks if they do occur?
What factors might increase or decrease risk?

What is the potential likelihood of the risks happening?

Documentation of this step

Explanation of the method used, and the definitions of the terms used to analyse the likelihood and consequences of each risk.

Rationale for initial screening of very low risks.

For all other risks:
existing control;
severity of consequences (with or without the control);
likelihood of occurrence (with or without the control); and
resulting level of risk.

Documentation should reflect the requirement for records to be relevant to the level of risk.

Evaluate risks

ISO 31000:2009	**5.4.4 RISK EVALUATION** … Risk evaluation involves comparing the level of risk found during the analysis process with risk criteria established when the context was considered. Based on this comparison, the need for treatment can be considered….

This step is about deciding whether risks are tolerable or unacceptable. A risk is called tolerable if it is not going to be treated in step 5.5. Defining a risk as tolerable does not imply that the risk is insignificant.

The evaluation should take account of the degree of control over each risk and the cost impact, benefits and opportunities presented by the risks. Also, the risks borne by other stakeholders that benefit from the risk should be considered.

The significance of the risk and the importance of the policy, program, process or activity need to be considered in deciding if a risk is tolerable.

A risk may be tolerated if the consequence and likelihood of that risk is consistent with the established criteria. These criteria should have established the threshold of what, for the organisation, would constitute an unacceptable exposure. The ability of the organisation to absorb an incident will, to a large degree, depend on the size and "financial health" of that organisation.

Reasons why a risk may be tolerated

- The opportunities presented outweigh the threats to such a degree that the risk is justified.
- The level of the risk is so low that specific treatment is not appropriate within available resources.
- The risk is such that there is no treatment available. For example, the risk that a project might be terminated following a change of government is not within the control of an organisation.
- The cost of treatment, including insurance costs, is so manifestly excessive compared to the benefit that toleration is the only option. This applies particularly to lower ranked risks.

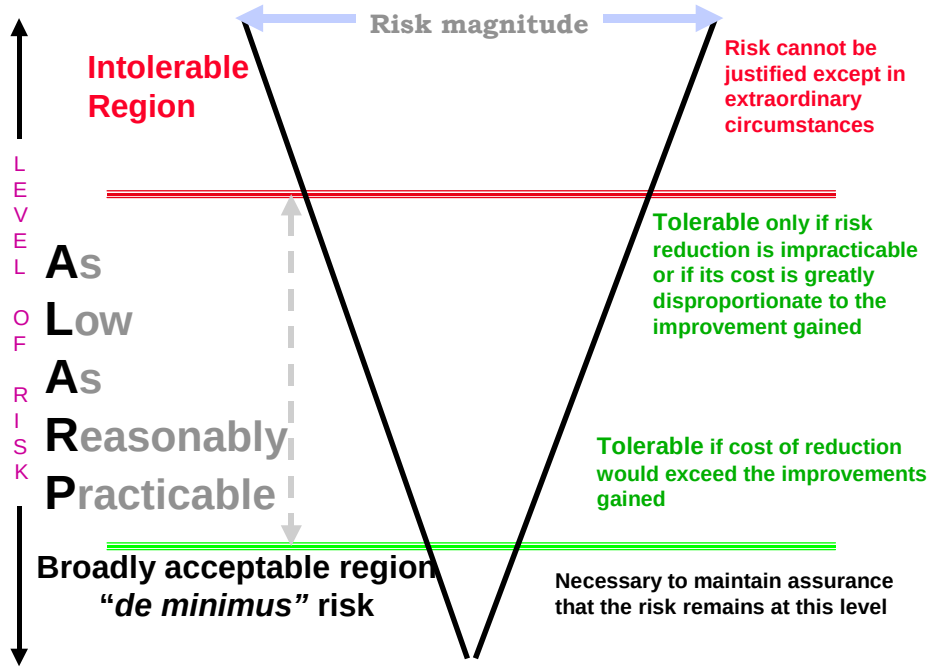
One approach is to compare the level of each risk, from the analysis step, against the level of tolerable risk assessed from Step 5.3 (Establishing the Context). A review of the risk criteria from Step 5.3.5 may be needed to ensure that criteria have been identified for all significant risks.

The risks not considered acceptable are those which will be treated in some way. These are prioritised for subsequent management action as a component of the organisations action plans.

As Low As Reasonably Practicable

The **as low as reasonably practical** (ALARP) concept is illustrated below. The width of the cone indicates the size of risk. In general two criteria can be defined. A level where risk is negligible and can be accepted without specific treatment other than monitoring and a level where risk is intolerable and the activity must cease, unless risk can be reduced. Between these levels is a region where costs and benefits are taken into account. When risk is close to the intolerable level the expectation is that risk will be reduced unless the cost of reducing the risk is grossly disproportionate to the benefits gained. Where risks are close to the negligible level then action may only be taken to reduce risk where benefits exceed the costs of reduction.

Associated concepts are as low as reasonably achievable (ALARA), which is based on a balance of cost and benefit, and De minimus which ignores the cost of treatment in seeking to achieve a trivial or insignificant level of risk.



The ALARP Principle

Interpretation of 'Reasonably Practicable'

The *Queensland Workplace Health and Safety Act 1989* provided the following definition of 'practicable'.

…"**practicable**", where the context permits, means practicable having regard to:

(a) the nature of the employment or, as the case may be, the particular aspect of the employment concerned;

(b) the severity of any potential injury or harm to health or safety that may be involved, and the degree of risk that exists in relation thereto;

(c) the state of knowledge about the injury or harm to health or safety that may be involved , about the risk of that injury or harm to health or safety occurring and about any ways of preventing, removing or mitigation that injury, harm or risk;

(d) the availability and suitability of ways to prevent, remove or mitigate that injury or harm to health or safety or risk; and

(e) whether the cost of preventing, removing or mitigating that injury or harm to health or safety or that risk is prohibitive in the circumstances.'

A legal opinion from a Barrister active in the OH&S area in Victoria provides the following definition of '**reasonably practicable**'.

> ' "Reasonably practicable" having regard to:
> (a) the severity of the hazard or risk in question;
> (b) the state of knowledge about that hazard or risk and any ways of removing or mitigating that hazard or risk;
> (c) the availability and suitability of ways to remove or mitigate that hazard or risk; and
> (d) the cost of removing or mitigating that hazard or risk.
>
> This definition relates to the duties imposed in the Act. It means **ALL** these factors must be taken into account when determining whether the duty has been met rather than only looking at any single factor, e.g. cost.'

However, the following opinion given by Lord Justice Asquith in 1949 is offered as the cleanest and simplest definition of our duty to do things in so far as is reasonably practicable. If we base our decisions on the following definition then we will have a strong argument to suggest we have discharged our duty of care.

> ' "**Reasonably practicable**" is a narrower term than "**physically possible**" and it seems to me to imply that a computation must be made by the owner, in which the quantum of risk is placed on one scale and the sacrifice involved in the measures necessary for averting the risk (whether in money, time or trouble) is placed in the other; and that if it be shown that there is a gross disproportion between them — the risk being insignificant in relation to the sacrifice — the defendants discharge the onus on them. Moreover, this computation falls to be made by the owner at a point of time anterior to the accident. (Edwards v National Coal Board (1949) 1 KB 704 at 712, CA, per Asquth LJ)'

Key questions in assessing and ranking

- What is the tolerable level of risk?
- What is the priority of the risks (eg., high, medium, low)?

Documentation of this step

- Consideration of tolerability criteria if not done previously.
- List tolerable risks with the reasons they are considered acceptable.
- List intolerable/unacceptable risks in priority order.

Treat risks

ISO 31000:2009	**5.5.1 General** Risk treatment involves selecting one or more options for modifying risks, and implementing those options. Once implemented, treatments provide or modify the controls.

This step is about considering options for treating risks which were not considered tolerable at the previous step. A combination of options may be appropriate in treating risks:

The criteria affecting the level of funding for treating risks should be established at the outset of the risk management process within the framework of the strategic, organisational and risk management context. **(Section 5.3 of ISO 31000:2009).**

Following risk evaluation, the various treatment options available should be identified. **(Section 5.5.2 of ISO 31000:2009).**

Identifying options for Risk Treatment

These may include:

Avoiding the risk by deciding either not to proceed with the activity that contains an intolerable risk (if this is practicable), choosing an alternative more tolerable activity which meets the objectives and goals of the organisation, or choosing an alternative less risky methodology or process within the activity.

The option of adopting an alternative work practice of lower risk reduces the consequences and/or likelihood of harm or loss and therefore, is a treatment and not necessarily avoidance of risk. Avoiding the risk is equivalent to refusing to accept the risk.

Reducing the likelihood or the consequences of the risk, or both. Note that there is a trade off between the level of risk and the cost of reducing those risks to an acceptable level. As already stated, the acceptable level should be consistent with the established risk criteria. (The relationship between risk and the cost to reduce a particular risk is shown in the figure on the next page).

Any one of several decision points may be chosen. These include:

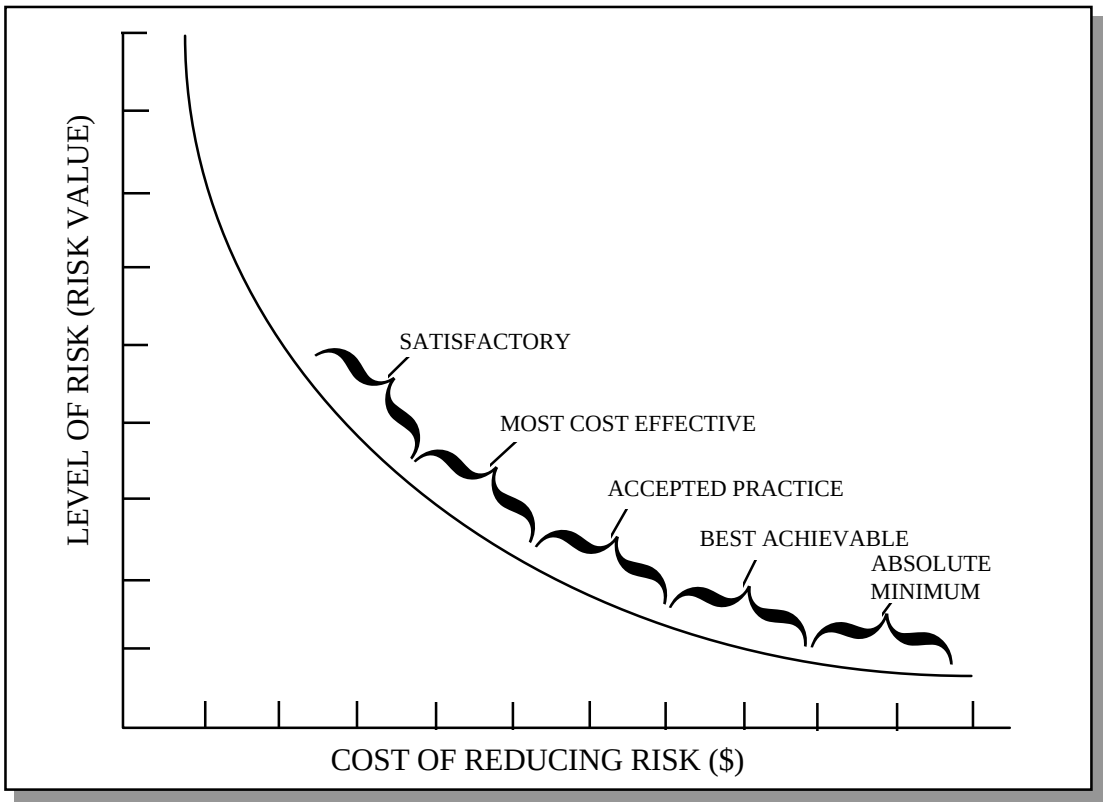
a satisfactory (but not optimum) solution;
the most cost-effective solution;
the accepted practice (industrial norm, good business practice);
the best achievable result (given current technology); and
the absolute minimum.

Which criterion is considered to be the most acceptable, depends on the circumstances and the established risk context within which the decision has to be made. With the right scenario, a valid argument can be made for any of the above options.

Where risk reduction is considered both feasible and cost effective, the required funding will need to be budgeted, with the responsible person ensuring that the risk reduction measures are carried out to the level determined.

Sharing the risk, in full or in part, with another party, preferably by mutual consent. From a Public Sector perspective, this could mean sharing it with the public at large and, in many instances, this may be unacceptable for political, moral or constitutional reasons. Again, the risk criteria should establish the level of tolerability of risk sharing. Where risks are shared in whole or in part, the organisation transferring the risk has acquired a new risk, in that the organisation to which the risk has been transferred may not manage the risk effectively.

Retention of either residual risks, following completion of risk reduction measures; those risks which, for political, moral or constitutional reasons are required to be retained by Public Sector organisations; or risks that have not been identified.



The Trade-off Between Level of Risk and Cost of Reducing Risk

Continually Monitor and Review

ISO 31000:2009	**5.6 MONITORING AND REVIEW** Both monitoring and review should be a planned part of the risk management process and involve regular checking or surveillance. It can be periodic or *ad hoc*.

Monitoring and review is an essential and integral step in the process for managing risk. It is necessary to monitor risks, the effectiveness of the plan, strategies and management system that have been set up to control implementation of the risk treatments.

Risks need to be monitored periodically to ensure changing circumstances do not alter the risk priorities. Few risks remain static.

Programs and processes change, as can the political, social and legal environment and goals of an organisation. Accordingly, it is necessary to re-examine the risk context to ensure the way in which risks are managed remain valid.

The principles of risk management are quite general in nature, but their application depends upon the context and environment from time to time. The process of review and monitoring ensures that risk management strategies continue to be a vital part of the organisation's business processes. The presence of regular performance information can assist with identifying likely trends, trouble spots and other changes which have arisen.

Possible methods of review

internal check program;
internal audit;
external audit - Auditor General, independent audit;
external scrutiny - Ombudsman, Parliamentary or Council Committee,
Appeal Tribunals; Courts; Commissions of Inquiry;
physical inspections;
program evaluation; and
reviews of organisational policies, strategies and processes.

Key questions

Do the performance indicators address the key success elements?
Are the assumptions, including those made in relation to the environment, technology and resources, still valid?
Are the risk treatments effective in minimising the risks?
Are risk treatments comparatively efficient/cost effective in minimising risks?
Are the management and accounting controls adequate?
Do the risk treatments comply with legal requirements, government and organisational policies, including access, equity, ethics, accountability?
How can improvements be made?

Documentation of this step

Implementation review plan.
Review and evaluation plan.

Develop appropriate records

ISO 31000:2009	**5.7 Recording the risk management process** Risk management activities should be traceable. In the risk management process, records provide the foundation for improvement in methods and tools, as well as in the overall process.

Reasons for adequate records

demonstrates process conducted properly;
enables sharing and communication of information;
facilitates monitoring and review;
provides a record of risks;
provides accountability tool; and
provides an audit trail.

References:

The following documents are available online from: http://infostore.saiglobal.com/store/

AS/NZS ISO 31000:2009 Risk management — Principles and guidelines

ISO Guide 73:2009 Risk management — Vocabulary

ISO/IEC 31010:2009 Ed. 1.0: Risk Management - Risk Assessment Techniques

AS/NZS 5050:2010 Business continuity—Managing disruption related risk

AS 8000-2003 Corporate Governance Standards Set (Contains 8000, 8001, 8002, 8003 & 8004 and associated Handbooks). ***Standards Australia.***

SAA/NZS HB 246 (Rev):2010 Guidelines for Managing Risk in Sport and Recreation, ***Standards Australia/Standards New Zealand, 18 August 2010***

SAA HB 266:2010 Guide for managing risk in Not-For-Profit organisations, ***Standards Australia,13 August 2010***

SAA/NZS HB 327:2010 Communicating and consulting about risk, ***Standards Australia /Standards New Zealand, ISBN 978-0-7337-9346-2, Standards Australia, 2010***

The following Handbooks have been revised to bring them into harmonisation with AS/NZS ISO 31000:2009 and will eventually be available online from: http://infostore.saiglobal.com/store/

SAA HB 141-2010 Risk Financing Guidelines, ***Standards Australia.***

SAA HB 158-2010 Delivering assurance based on AS/NZS ISO 31000:2009 Risk Management, ***Standards Australia.***

SAA/NZS HB 203:201X Environmental risk management – Principals and process, ***Standards Australia/Standards New Zealand.***

The following Handbooks are currently being revised to bring them into harmonisation with AS/NZS ISO 31000:2009: -

SAA HB 205-201X OHS Risk Management Handbook, ***Standards Australia.***

SAA HB 436-201X Risk Management Guidelines – A Companion to AS/NZS ISO 31000:2009, ***Standards Australia/Standards New Zealand.***

The following Handbooks based on the superseded AS/NZS 4360:2004 require revision to bring them into harmonisation with AS/NZS ISO 31000:2009: -

HB 167:2006 - Security risk management, ***Standards Australia/Standards New Zealand.***

SAA HB 231:2004 Information Security Risk Management Guidelines, ***Standards Australia.***

SAA HB 240-2004 Guidelines for Managing Risk in Outsourcing using the AS/NZS 4360:2004 Process, ***Standards Australia.***

SAA HB 254-2005 Governance, risk management and control assurance, ***Standards Australia.***

SAA/NZS 221:2004 Business Continuity Management, ***Standards Australia/Standards New Zealand.***

SAA HB 292:2006 A Practitioners Guide to Business Continuity Management ***Standards Australia (2006)***

SAA HB 293:2006 An Executive Guide to Business Continuity Management ***Standards Australia (2006)***

SA HB 296:2007 Legal Risk Management, ***Standards Australia (2007), ISBN 0 7337 8295 7.***

Further Reading

Recent publications: ***http://www.riskworld.com/BOOKS/topics/riskmana.htm*** **and** ***http://www.amazon.com*** **and search under "risk management"**

Accident and Design – Contemporary Debates in Risk Management, Hood, Christopher & David K.C. Jones, Eds. (1996), London: UCL Press.

Against the Gods: The Remarkable Story of Risk, Bernstein, Peter L. ISBN 0-471-12104-5

Applying Risk Management Techniques to Complex Procurement, Cooper, DF (1997) Purchasing Australia, Australian Government Publishing Service, Canberra. ISBN 0 642 26803 7.

Democracy in Practice – Public Participation in Environmental Decisions, Beierle, Thomas C. & Jerry Cayford (2002) Washington: Resources for the Future.

Democratising Technology – Theory and Practice of a Deliberative Technology Policy, von Schomberg, Rene, Ed. (1999), Hengelo/Buenos Aires: International Centre for Human and Public Affairs.

Enterprise Risk Management - from Incentives to Controls, James Lam (2003), John Wiley & Sons, Chichester

Enterprise Risk Management - A Manager's Journey, K H Spencer Pickett, (2006), John Wiley & Sons, Chichester

Environmental Risk Assessment: An Australian Perspective, Beer, T and F Ziolkowski (1995) Supervising Scientist Report 102, AGPS, Canberra, ACT. ISBN 0 642 24301 8. (See www.erin.gov.au/portfolio/epa/pubs/risk_toc.html.)

Financial Risk Management: A Practitioner's Guide to Managing Market and Credit Risk (with CD-ROM), **Steve L. Allen (2003)**

Financial Risk Manager Handbook (Wiley Finance), **Philippe Jorion and GARP (Global Association of Risk Professionals) (2009)**

Globalization and the Environment – Risk Assessment and the WTO, Robertson, David & Aynsley Kellow, Eds. (2001), Cheltenham, UK: Edward Elgar.

Guidelines for Ecological Risk Assessment, Environmental Protection Agency (1998) Risk Assessment Forum, US EPA, Washington, DC, EPA/630/R-95/002F. (See www.epa.gov/ncea/ecorsk.htm.)

Guidelines for Managing Risk in the Australian Public Service, Commonwealth of Australia (1996) MAB/MIAC Report 22, AGPS, Canberra. ISBN 0 642 25236 X.

Handbook of Cost-Benefit Analysis, Australia Department of Finance. (1991). Australian Government Publishing Service, Canberra. ISBN 0 644 149159

Identifying and Managing Project Risk: Essential Tools for Failure-Proofing Your Project, Tom Kendrick PMP (2009)

In the Chamber of Risks – Understanding Risk Controversies, Leiss, William (2001) Montreal & Kingston: McGill-Queen's University Press.

Integrated Risk Management – Implementation Guide, Treasury Board of Canada Secretariat (2004) ISBN 0 662 65673 3. Available through: http://www.tbs-sct.gc.ca

Managing Risk in Procurement - A Handbook, DAS/Purchasing Australia 10.10.96,

Managing Risk, Waring, A and Glendon, A I (1998) International Thomson Business Press, London. ISBN 1 86152 167 7.

Managing Risks in Public Organisations, Martin Fone and Peter C. Young; August 2006; ISBN 1899287760

Multi-Level Risk Assessment, New South Wales Government (1999), Department of Urban Affairs and Planning, Sydney, NSW: Revised Edition. ISBN 0 7347 0062 8.

Non-stop service (Continuity Management Guidelines for Public Sector Agencies), Emergency Management Australia 1997, ISBN 0 642 28329 X

Pipeline Risk Management Manual, Muhlbauer, WK (1996) Gulf Publishing, Houston: Second Edition. ISBN 0 88415 668 0.

Practical Risk Assessment for Project Management, Grey, S (1995) John Wiley & Sons, Chichester. ISBN 0 471 93979 X.

Principles of Communicating Risks, Mulligan, Jean, Elaine McCoy, and Angela Griffiths, (1998), The Macleod Institute for Environmental Analysis, University of Calgary, Calgary, Alberta

Project Risk Management: Processes, Techniques and Insights, Chapman, CB and Ward, SC (1997) John Wiley & Sons, Chichester. ISBN 0 471 95804 2.

Quantitative Risk Analysis: A Guide to Monte Carlo Simulation Modelling, Vose, D (1996) John Wiley & Sons, Chichester. ISBN 0 471 95803 4.

Quantitative Risk Management: Concepts, Techniques, and Tools (Princeton Series in Finance)**, Alexander J. McNeil, Rudiger Frey, and Paul Embrechts (2005)**

Reputational Risk: Responsibility Without Control?, Derek Atkins, Ian Bates, and Lynn Drennan (2006)

Risk Analysis and Society – An Interdisciplinary Characterization of the Field, McDaniels, Timothy & Mitchell J. Small, Eds. (2004), Cambridge: Cambridge University Press.

Risk and Crisis Management in the Public Sector (Routledge Masters in Public Management), Lynn Drennan and Allan McConnell (2007)

Risk and Rationality – Philosophical Foundations for Populist Reforms, Shrader-Frechette, K.S. (1991), Berkeley: University of California Press.

Risk Governance: Towards an Integrative Approach, Renn, Ortwin with Annexes by Peter Graham (2005) IRGC, Geneva (http://www.irgc.org/_cgidata/mhscms/_images/12326-3-3.pdf)

Risk Management, Michel Crouhy, Robert Mark, and Dan Galai (2000)

Risk Management Guide for DoD Acquisition, Department of Defence (1998) Defence Acquisition University, Defence Systems Management College, VA

Risk Management: Changing the Internal Auditor's Paradigm, McNamee, David & Selim, Georges (1998), The Institute of Internal Auditors Research Foundation, USA,

Risk Management's Role in Corporate Governance, Boyd, J., Corporate Risk, Vol. 4, No. 8, August 1997

Risk Management, Tricks of the Trade for Project Managers, Rita Mulcahy (2003)

Risk: Analysis, Assessment and Management, Ansell J and F Wharton (Eds) (1992), John Wiley & Sons, Chichester. ISBN0 471 93464 X.

Risk Quantification: Management, Diagnosis and Hedging (The Wiley Finance Series), Laurent Condamin, Jean-Paul Louisot, and Patrick Naïm (2007)

Risky Business – Canada's Changing Science-Based Policy and Regulatory Regime, Doern, Bruce G. & Ted Reed, Eds. (2000) Toronto: University of Toronto Press.

Safe Enough? Managing Risk and Regulation, Jones, Laura, Ed. (2000) Vancouver: The Fraser

Institute.

Simple Tools and Techniques for Enterprise Risk Management, Robert J Chapman, (2006), John Wiley & Sons, Chichester

The Essentials of Risk Management, Michel Crouhy, Dan Galai, Robert Mark, and Michel Crouhy (2005)

The Failure of Risk Management: Why It's Broken and How to Fix It, Douglas W. Hubbard (2009)

The Fundamentals of Risk Measurement, Christopher Marrison (2002)

The Government of Risk – Understanding Risk Regulation Regimes, Hood, Christopher, Henry Rothstein & Robert Baldwin (2001) Oxford: Oxford University Press.

Whack-a-Mole: The Price We Pay for Expecting Perfection, David Marx; August 2009; ISBN-10 0615283071; ISBN-13 978-0615283074

Specific Information on Risk Analysis

Society for Risk Analysis (SRA) at: http://www.sra.org

Web Sites

Australian & International Standards: -
http://www.saiglobal.com/shop/Script/portal.asp?portal=RiskManagement

Australian National Audit Office: - ***www.anao.gov.au (visit "Best Practice Guides", "Speeches" & "Reports" – search under 'risk Management'.)***

Emergency Management Australia: - ***www.ema.gov.au***

Institute of Internal Auditors: - ***www.theiia.org/home.htm***

New South Wales Audit Office: -
http://www.audit.nsw.gov.au/perfaud-rep/RiskManagement-June2002/Risk-Contents.html

Queensland Audit Office – Report No. 7 for 1998- 99: Corporate Governance Beyond Compliance: -
http://www.qao.qld.gov.au/pages/publications/pub_ag.html

Queensland Audit Office – Report No. 1 for 2001- 02: Incorporating a Review of Corporate Governance -
http://www.qao.qld.gov.au/pages/publications/pub_ag.html

Queensland Audit Office – Report No. 6 for 2007: ***Beyond Agency Risk*** **-**
http://www.qao.qld.gov.au/pages/publications/pub_ag.html

The Society for Risk Analysis: - ***www.sra.org***

Treasury Board of Canada: - ***http:www.tbs-sct.gc.ca/rm-gr***
EACSR (2004): External Advisory Committee on Smart Regulations, *Smart Regulation – A Regulatory Strategy for Canada.*
Available at: ***http://www.pco-bcp.gc.ca/smartreg-regint/en/index.html***

UK Auditor General: - ***http://www.nao.gov.uk/publications/nao_reports/9900864.pdf***

UK Cabinet Office: - http*://www.strategy.gov.uk*
Strategy Unit (2002) *Risk: Improving government's capacity to handle risk and uncertainty*.
Strategy Unit of the UK. Available at: ***http://www.strategy.gov.uk/downloads/su/RISK/REPORT/01.HTM***

UK Government: - ***http://www.risk-support.gov.uk***

UK Treasury: - ***http://www.hm-treasury.gov.uk***
HM Treasury (2004) *The Orange Book. Management of Risk: Principles and Concepts*.
Available at:
http://www.hm-treasury.gov.uk/d/orange_book.pdf

HM Treasury (2005) *Managing Risks to the Public: Appraisal Guidance*.
Available at: ***http://www.hm-treasury.gov.uk/media/8AB/54/Managing_risks_to_the_public.pdf***