Session No. 712

"The Significance and Impact of New International Risk Management Standards"

J.F. (Jim) Whiting, MSc, Dip.Ed., CPEng, SMIE(Aust)
Managing Director, Principal Risk Engineer
risk@workplaces pty ltd
Brisbane, Australia

Introduction

This paper describes how finalization of the three new international standards: (1) ISO 31000, *Risk Management- Principles and guidelines on implementation;* (2) ISO/IEC 31010, *Risk management- Risk assessment guidelines;* and (3) ISO/IEC Guide 73, *Risk Management- Vocabulary* represents a significant development in the world of managing all risks, not only health and safety risks. Based on the best of existing national standards, the new standard provides the much awaited international consistency in terminology, principles and methods of risk management. As such, the new standards minimize confusion among users regarding terminology, practical interpretation and structured implementation of risk management systems throughout the world.

Why Risk Management?

In the face of ever-present uncertainty, risk management is fundamentally about how well an organization can CONSISTENTLY understand / manage opportunities to exploit and associated threats that can confront it in meeting OR not meeting its objectives.

For all decision-making throughout an organization, particularly during planning and managing change, risk management needs to be embedded into every aspect of management processes. As such, risk management is core to ALL "modern" management. Any decision making related to managing work safety and health risks needs to involve the explicit application of risk management principles and techniques. This ensures that OHS risks are reduced to a degree that is morally, legally, and commercially appropriate to the nature of the risks. Corporate governance, compliance and due diligence depend on being able to demonstrate both a strong understanding of risks and appropriate means of successfully managing them.

There are significant advantages of incorporating harmonized practices throughout all aspects of risk management. The resulting improvements in consistency in management processes and practices return legal and commercial benefits. Consistency need not imply absolutely rigid uniformity. Internally, different risk "domains" e.g., OHS/Environment/Financial, may still require uniqueness in some aspects such as Consequence scales and risk tolerability criteria. However, traditional "silos" or "empires" cannot justify the continuation of managing their risks in different ways. Uniqueness is often over-stated and wasteful.

Externally, organizations also see the value of being able demonstrate at all levels—clients/industry-wide/nationally/internationally—that their management systems conform to international standards (see Figure 1).

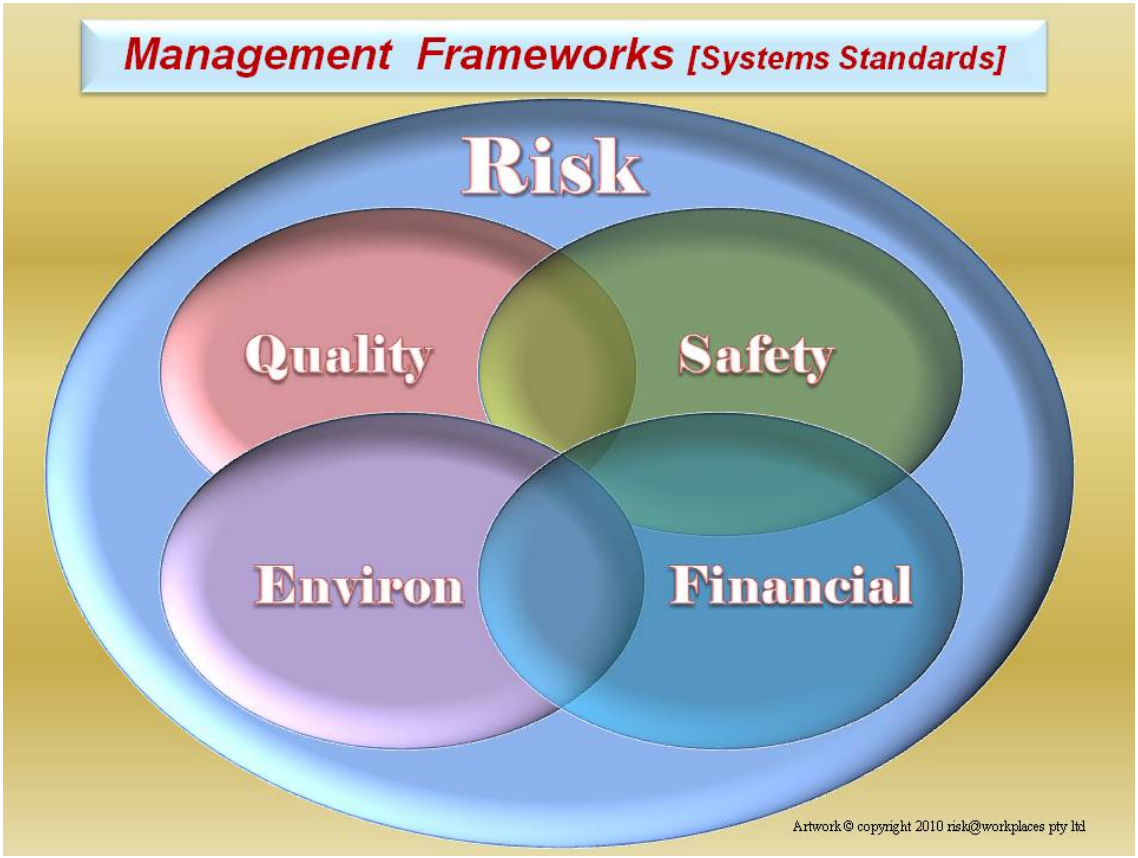


Figure 1. A Risk Management Framework provides a universal binding envelope to achieve corporate-wide consistency in systems and processes throughout all aspects of management.

Risk management needs to be formally applied when options are being proposed, evaluated, and selected, before as well as after decisions are made. Application of risk management can never be simply an after-thought, or simply buying insurance. There is never complete *risk transfer* rather *risk sharing*. Risk management principles and considerations are essential in management decision-making such as choosing between risk control options for managing any kind of risk as in Figure 2.

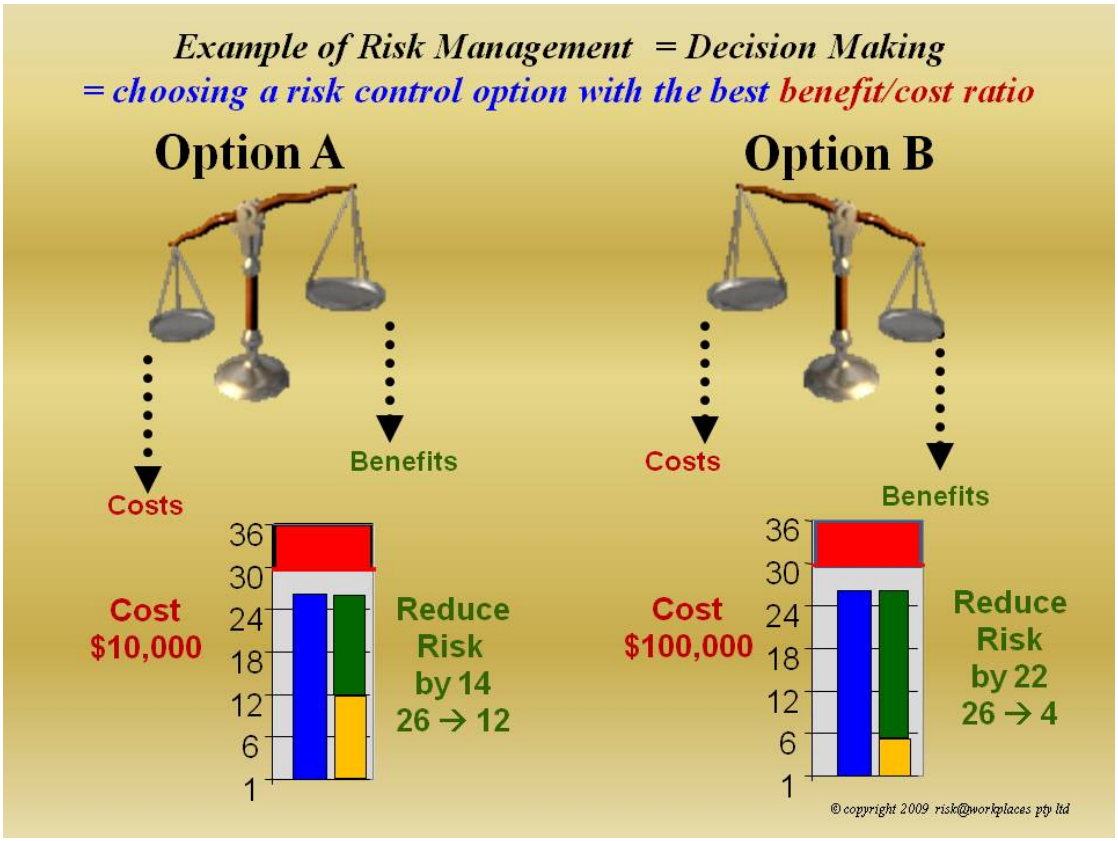


Figure 2. Decision-making—for example deciding between risk control options during one form of risk treatment—requires fundamental risk management processes such as comparative cost-benefit analyses and applying "reasonably practicable" criteria. (Also see Appendix 2)

Other examples of risk management being valuable in management processes include more objective definitions of a manager's expectations re risk-taking behaviors during employee inductions before incidents and also counseling after incidents. Risk scoring can assist the process of optimizing the alignment between managerial and employee risk perceptions. *Quote – "If we calculate together the risk of doing it your way, do you agree that the risk level is 18 on say a 36 point log scale and do you also agree that our calculation of the corresponding risk level of doing it the agreed company way is 6 on the same scale. Therefore, are you convinced that the agreed company way - as the lowest tolerable risk level- is to be followed from now on ?".* Usually a fair and just culture includes the proviso that - If this process of aligning perceptions of tolerable risk after an incident doesn't work in 3 attempts, *"then we can't achieve alignment of agreed perceptions of what is tolerable and therefore someone has to leave and it is not me !"*

There is a strong argument for the inclusion of objective risk assessments whenever safety is being discussed anywhere, anytime. Every discussion of "safe" and "safety" needs consistent **standardized** objective risk assessment we will continue to suffer from subjective confusion and lack of agreement between *"safe"* meaning *"zero risk"* or *"risk managed to as low as reasonably practicable ALARP "*

Overview of ISO31000

The development of the new international standards has built on a number of international standards, guidelines and codes as in Figure 3:

- ISO 31000:2009 Risk management — Principles and guidelines on implementation
- ISO/IEC 31010:2009 Risk management – Risk assessment guidelines
- AS/NZS 4360:2004 Risk Management
- BS 31100:2008 –Risk Management Code of practice
- ISO 17776:2000 Petroleum - LNG industries – Risk Assessment
- IEC 61508-2000 Functional Safety
- NIST Standards & Risk Management Framework
- ANSI B11.TR3 Risk reduction (Machine tools)
- Mil Std882D: 2000-DoD-Standard – System Safety
- OSHA PSM 1910 119 Process Safety Management Rule
- CSA Q850 – 1997 Risk management – Guideline for Decision-Makers
- NORSOK Z-013-2001- Risk emergency preparedness
- COSO 2004 Enterprise Risk Management ERM Integrated Framework

Figure 3. The development of the new standards has built on a number of international standards, guidelines and codes.

While most standards in the past have emphasized **Process only**, the new ISO 31000 standard provides all three components - **Principles** and **Framework** as well as **Process** (see Figure 4). As such it provides comprehensive assistance to an organization to establish a structured approach to integrating risk management as its over-arching management system. Organizations can adapt the components of the **Framework (see** Figure 5) to their specific needs. Many PDCA-type frameworks are compatible with this. The language / terminology do not need to be slavish copies of those in Figure 5. If an organization's existing management practices and processes include components of risk management or if the organization has already adopted a formal risk management structure and process for particular types of risk or situations, then these can be critically reviewed and assessed against this International Standard as the basis for determining adequacy and governance. Among the **Principles** of ISO 31000, Enterprise Risk management ERM is about creating value out of uncertainty anywhere in the organization, during any activities to achieve any of its objectives. One significant aspect of ISO 31000 is standardization of the risk management **Process,** Figures 6A and 6B). Now any organization can use a consistent, structured process for managing any kind of risk for any aspect of its activities and business. Note that in Figures 6A and 6B, ISO 31000 continues the emphasis on *Establishing the Context, Scope* and *Risk Criteria* as the first step of a risk management process. Some individuals still wrongly believe that the first step in a risk management process is Risk Identification.

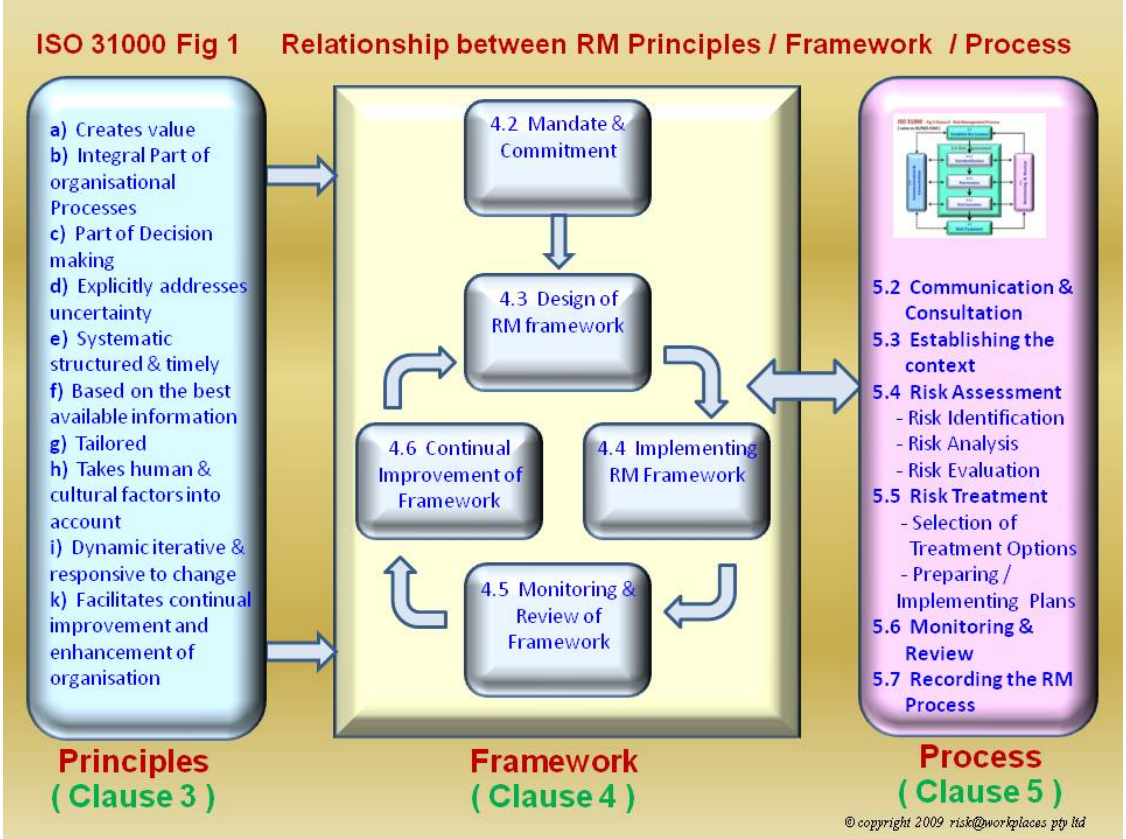


Figure 4. The emphasis is now also on the Principles and Framework as well as the traditional attention to only the Process of risk management.

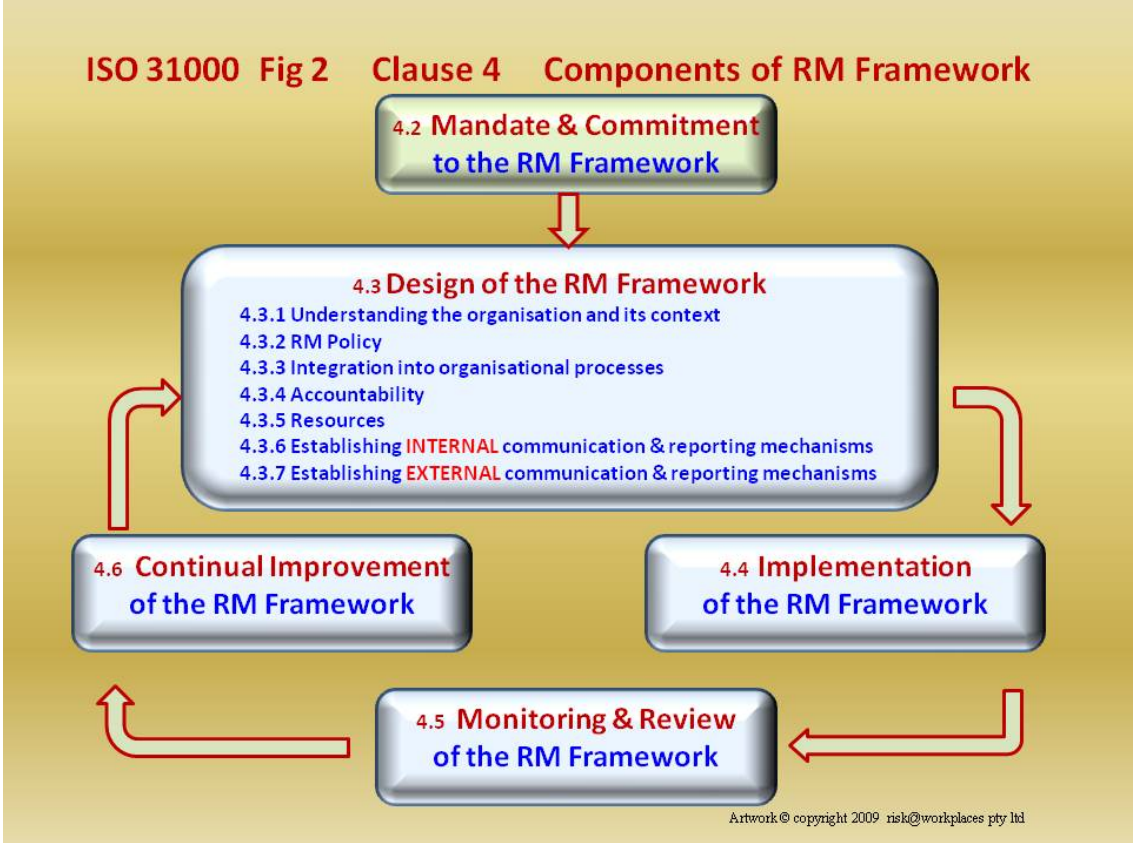


Figure 5. A traditional management framework is similar to "Plan Do Check Act" and others. Note the emphasis on Internal and External Communication and the never-ending loop of continuous improvement.

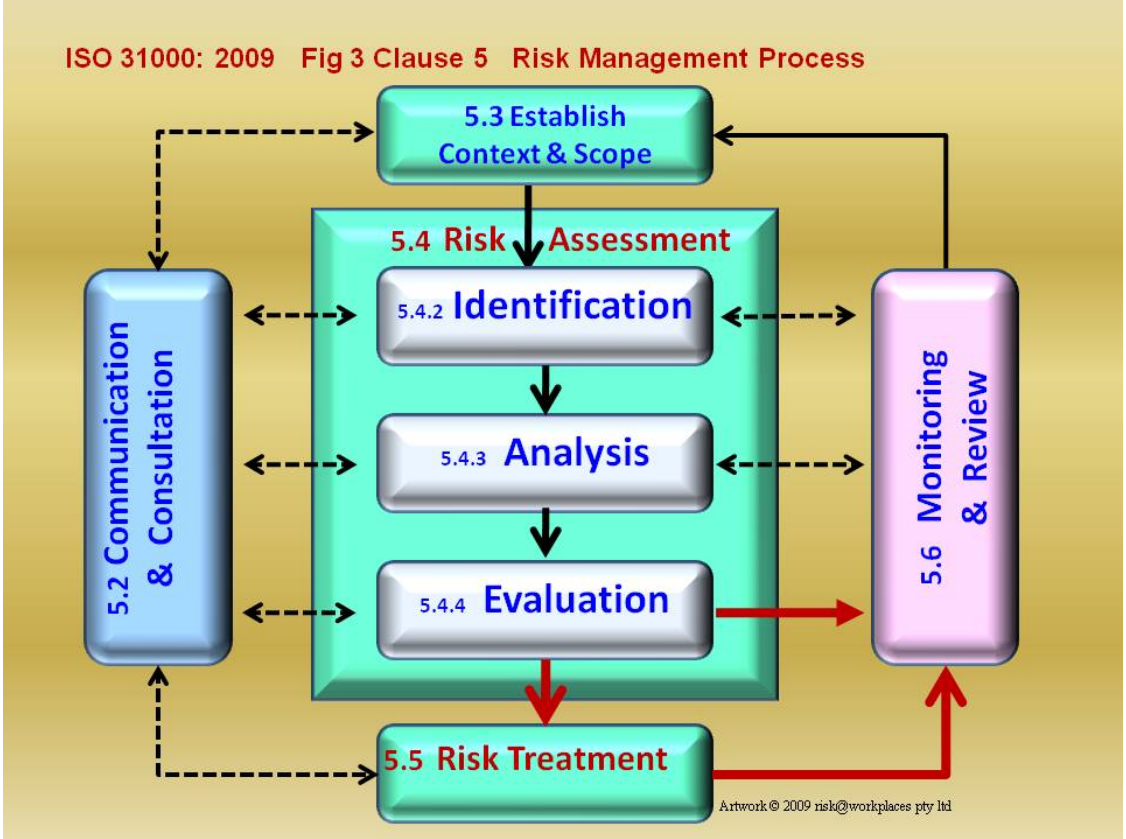


Figure 6A. The RM process in ISO31000 is similar to a number of existing International standards but with some significant changes in terminology, e.g. risk assessment

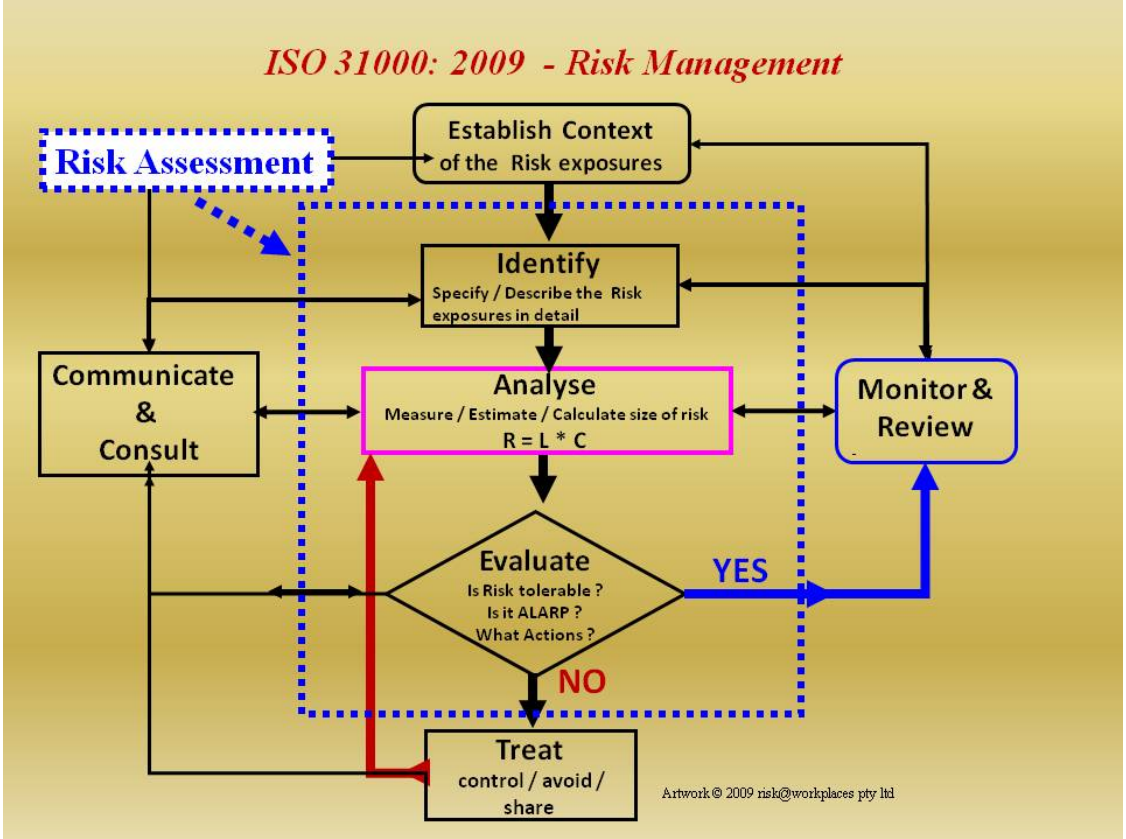


Figure 6B. The author's variation of Figure 3 in the standard in Figure 6A. The added emphasis is the detail in the risk evaluation / treatment phases of the process.

Generic Nature of ISO31000 Requirements

Risk Criteria

ISO31000 does not specify the exact details of all ways of meeting requirements. Rather it states clearly what elements of a risk management system are necessary without any specific "how" or "what". A good example is **Clause 5.3.5, Defining risk criteria.** Clause 5.3.5 is quoted in Appendix 1 of this paper. ISO31000 does not specify how each of the criteria elements in Clause 5.3.5 are to be defined and met, but simply says that they should be agreed at the highest level of policy-making in the organization and then formalized into a Risk Policy and Framework. Take the criterion in Appendix 1,*"how the level of risk is to be determined"*. ISO31000 is silent about the exact methods of risk analysis to be used – qualitative AND/OR semi-quantitative matrix AND/OR full quantitative risk analysis QRA. There is no "recommended" or "mandatory" 5×5 matrix of Likelihoods and Consequences, defined in the standard; but it does say that the organization needs to define which kinds of risk analysis will be used and when and how.

Reasonably Practicable

Another criterion in Clause 5.3.5 for when *"the level at which risk becomes acceptable or tolerable"* (see Figure 7A) is also a good example of the generic but nevertheless clear requirement of the standard. In actual fact, most organizations would not currently satisfy this requirement. Not many organizations are explicit about the criteria which managers are to apply

during risk evaluation and risk treatment. Some organizations can easily meet the standard with the use of risk tolerability policies and frameworks based on "reasonable and practicable" such as ALARP – As Low As Reasonably Practicable and SFARP – So Far as is Reasonably Practicable (see Figure 7B). The standard does not dictate how this criterion is to be satisfied. Regulators in different legal risk jurisdictions have developed objective ALARP criteria (see Appendix 2) and organizations adopting similar policy criteria are not only able to demonstrate that they are meeting their legal requirements but also can obtain assurance of appropriate moral and commercial governance.

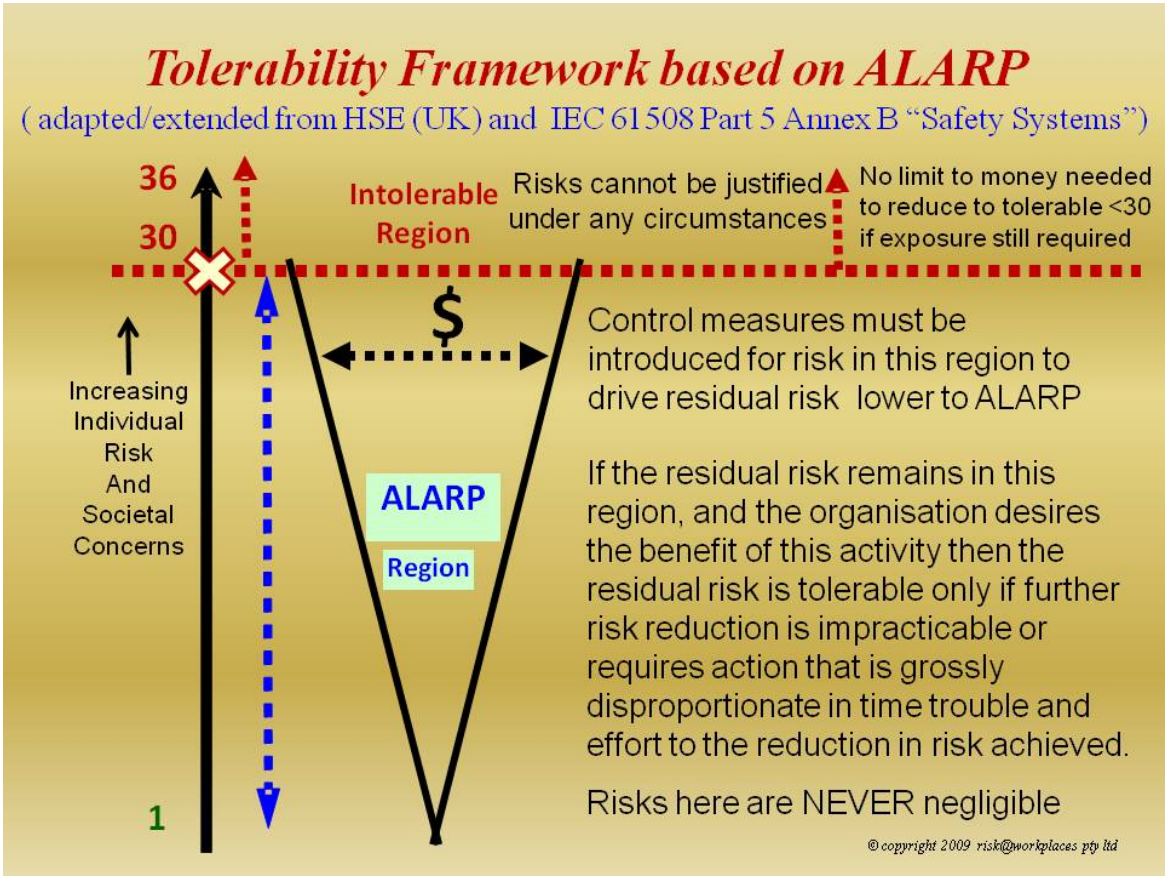
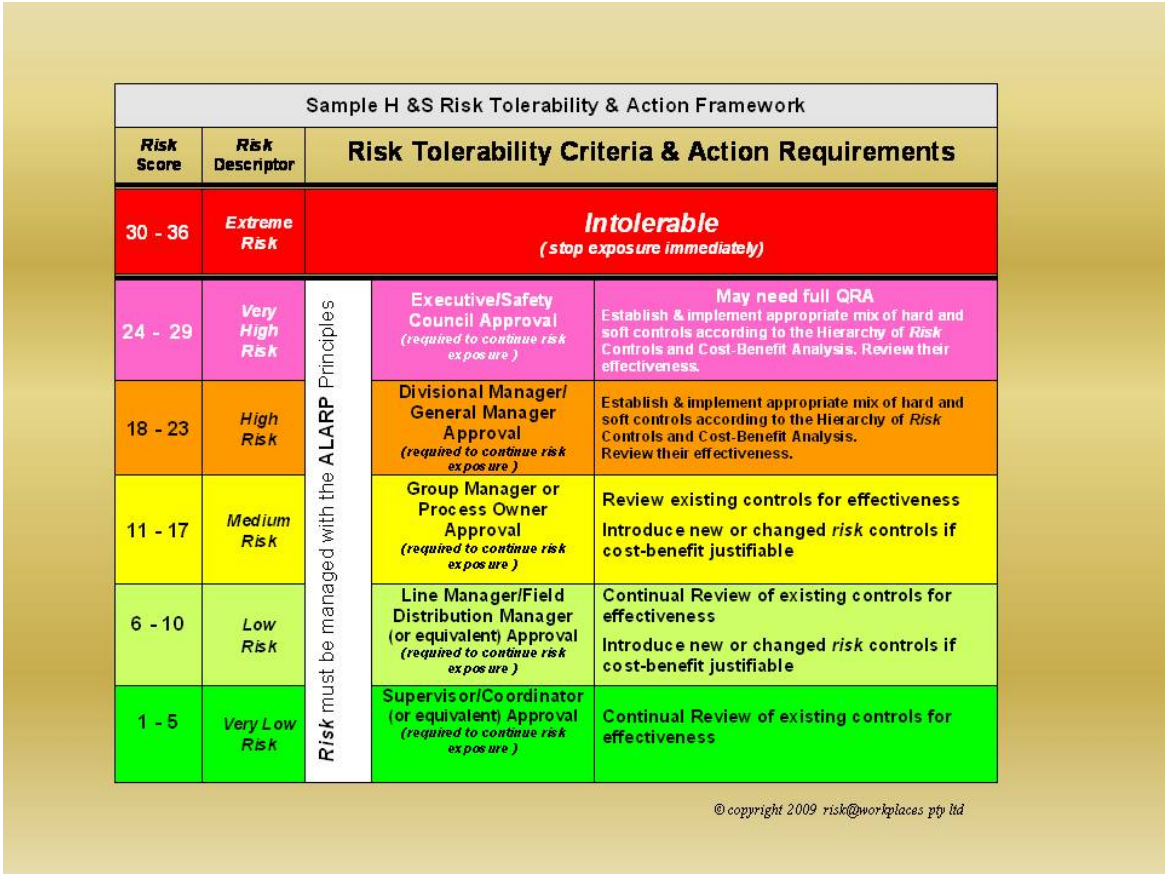


Figure 7A. This example of a Risk Tolerability Framework shows the organization's chosen criteria for evaluating risk, ISO31000 does NOT dictate this detail for the criterion in Clause 5.3.5 - when is the – *"the level at which risk becomes acceptable or tolerable"* but it requires equivalent policies and practices.



Sample H &S Risk Tolerability & Action Framework

Risk Score	Risk Descriptor	Risk Tolerability Criteria & Action Requirements		
30 - 36	Extreme Risk	Intolerable (stop exposure immediately)		
24 - 29	Very High Risk	Risk must be managed with the ALARP Principles	Executive/Safety Council Approval (required to continue risk exposure)	May need full QRA Establish & implement appropriate mix of hard and soft controls according to the Hierarchy of Risk Controls and Cost-Benefit Analysis. Review their effectiveness.
18 - 23	High Risk		Divisional Manager/ General Manager Approval (required to continue risk exposure)	Establish & implement appropriate mix of hard and soft controls according to the Hierarchy of Risk Controls and Cost-Benefit Analysis. Review their effectiveness.
11 - 17	Medium Risk		Group Manager or Process Owner Approval (required to continue risk exposure)	Review existing controls for effectiveness Introduce new or changed risk controls if cost-benefit justifiable
6 - 10	Low Risk		Line Manager/Field Distribution Manager (or equivalent) Approval (required to continue risk exposure)	Continual Review of existing controls for effectiveness Introduce new or changed risk controls if cost-benefit justifiable
1 - 5	Very Low Risk		Supervisor/Coordinator (or equivalent) Approval (required to continue risk exposure)	Continual Review of existing controls for effectiveness

Figure 7B. This example of a Risk Tolerability Framework shows the framework/policies of Figure 7A extended to include the organization's chosen criteria for assigning risk ownership and recommending risk treatment actions. All the criteria are naturally based on size and significance of the risk.

Assigning Risk Owners and Accountability

An important highlight of the new standard is the new emphasis on the "risk owners" and their accountabilities responsibilities and authorities. Clause 4.3.3 is shown in Appendix 4 of this paper. Organizations which already incorporate specific naming of "owners" of specific risks do not report unhealthy negative perceptions of managers as increased vulnerability. Rather the reverse situation exists - with managers welcoming a system of clarification of formal boundaries of responsibility. They are also comforted by the system allowing them a formal method to demonstrate positively that they are following processes and managing risks according to corporate criteria.

Implications for Organizations

Conformance or Certification?

As with all management standards, an organization can choose varying degrees of application of ISO31000. Even though ISO itself states (see Appendix 3 of this paper) that " *ISO31000 is not intended for the purpose of certification"*, a significant standard such as this now provides all organizations the opportunity to improve or establish effective risk management systems. While

the standard does not prescribe details of requirements with "shall" s it appropriately uses "should" s throughout. In fact, "should" appears 86 times in ISO 31000. For interest, the less prescriptive "can" appears 91 times.

The term "should" does indicate a requirement similarly to the term "shall". By addressing the each "should" requirement, it becomes straightforward to perform internal or external reviews / audits. In this way, conformance of an organization's own system with the stated desirable standard elements can be gauged.

For all its standards ISO does not dictate the need for an external accredited third party or agency to provide a formal certificate document that states the result of an external audit of conformance with requirements of the standard. Mature organizations with advanced risk management structures and systems can use conformance with the standard to provide internal assurance that they meet an international standard. These organizations would be interested in at least internal reviews / audits against each of ISO31000's requirements. Caution needs to be exercised to ensure that time, money, and effort are not wasted in changing existing RM system components artificially and unnecessarily because they may not have the exact appearance of elements of ISO31000. Many changes may need to be only minor or even cosmetic. Organizations with less mature RM systems will need to establish [sometimes with external advice] priorities for fixing non-conformances revealed by internal or external reviews / audits. According to a mature organization's Change Management Policies, that decision-making process like any change needs to follow the ISO31000 process itself. Will an "industry" of auditing and certification to ISO31000 develop in the near future ? The answer will be market-driven. If internal and external stake-holders believe that independent formal external assurance is necessary then naturally it will.

Integration of Risk Management Systems

Integration and consistency principles are often referred to by a number of terms :-
"A rose by any other buzz word"

- ►TRM Total Risk Management,
- ► IRM Integrated Risk Management,
- ► HRM Holistic Risk Management,
- ► ERM Enterprise Risk Management
- ► EWR Enterprise Wide Risk

Conforming with or following ISO31000 can provide organizations with an effective basis for **ERM Enterprise Risk Management** – managing risks in all risk domains in generic but consistent ways. As well as meeting ERM requirements, ISO31000 allows any necessary silo / project approaches to risk management. Many organizations have used The Committee of Sponsoring Organizations COSO II of the Treadway Commission as their basis for an effective ERM. They have been dissatisfied and disappointed because it is difficult to understand and implement. The new ISO31000 is a clearer, more mature and adaptable system standard.

ISO/IEC 31010

ISO31000 is supported by a tools / methods companion Standard **ISO / IEC 31010, Risk management — Risk assessment guidelines.** This international standard provides extensive guidance for the selection and application of systematic / methodical techniques for risk assessment. IEC 31010 details how tools and methods for risk assessment may be selected. The annexes list and further explain a very wide range of tools and techniques that can be used to

perform or assist with the risk assessment process. A list of heading from Part B.14) in IEC/ISO 31010 can be found in Figure 8. Figure 9 lists the risk assessment tools and methods covered in ISO/IEC 31010:2009:

B.14.1 Overview
B.14.2 Use
B.14.3 Inputs
B.14.4 Process
B.14.5 Outputs
B.14.6 Strengths and Limitations
B.14.7 Comparisons and Links
B.14.8 References

Figure 8. The headings from part B.14 Fault Tree Analysis (FTA) in IEC/ISO 31010 show the detailed guidance provided for each assessment tool covered.

Risk Assessment Tools and Methods covered in ISO/IEC 31010:2009	
Failure mode and effect analysis (IEC 60812)	LOPA
Failure mode, effect /criticality analysis (IEC 60812)	SWIFT
Fault tree analysis (IEC 61025)	Decision Tree
Hazard and operability studies (HAZOP) (IEC 61882)	Bow Tie Analysis
Reliability centered maintenance (IEC 60300-3-11)	Monte Carlo
Markov analysis (IEC 61665)	Root Cause Analysis
Human reliability analysis	HACCP
Preliminary hazard analysis	Environmental Risk Assessment
Event tree analysis	Scenario Analysis
Brainstorming	Business Impact Analysis
Structured or Semi-Structured Interviews	Cause & Consequence Analysis
Delphi Techniques	Cause and effect analysis
Checklists	Sneak Circuit Analysis
Consequence/Likelihood Matrix	Bayesian Analysis

Figure 9. A comprehensive range of Risk Assessment Methods is described in ISO/IEC 31010

In Table A1 of ISO/IEC 31010, applicability ratings for each of above methods are given in terms of :

SA = Strongly Applicable in each part of the Risk Assessment Process

A = Applicable in each part of the Risk Assessment Process

NA = Not Applicable in each part of the Risk Assessment Process

In Table A2, Factors influencing selection of risk assessment methods, there is a tabulation of all the attributes of the methods (see Figure 10). These attributes are described in terms of:

• the **complexity** of the problem and the methods needed to analyse it;

• the **nature and degree of uncertainty** of the risk assessment based on the amount of information available and what is required to satisfy objectives;

• the **nature of resources** needed to carry out the risk assessment with regards to degree of involvement by management, amount and level of expertise required to perform the risk assessment or data and cost. Each method is rated as **high, medium, or low** in terms of these attributes

Category	Examples
Look-Up Methods	Checklists / Preliminary Hazard Analysis
Creativity Methods	Structured Interview / Brainstorming / Delphi Technique / Structured What-if (SWIFT) / Human Reliability Analysis (HRA)
Scenario Analysis Methods	Root Cause Analysis (Single Loss Analysis) / Scenario Analysis / Environmental Risk Assessment / Business Impact Analysis
Top Event Analysis Methods	Fault Tree Analysis FTA / Event Tree Analysis ETA / Cause -Consequence Analysis / Cause –Effect Analysis
Functional Analysis Methods	FMEA / FMECA / RCM / Sneak / HAZOP
Controls Assessment Methods	LOPA Layers of Protection Analysis / Bow Tie Analysis
Statistical Analysis Methods	Markov / Monte Carlo / Bayesian

Figure 10. Methods and Tools are Categorized from Table A2 of ISO/IEC 31010

Conclusions - WHY Implement ISO31000 in Your Organization?

The following are some of the reasons that you should implement ISO 31000 in your company or organization:

- Increased consistency / reliability in decision-making
- Consistency in terminology and processes
- Confidence in exploiting opportunities and dealing with threats,
- Integrated enterprise wide risk management
- Improved safety, financial, and corporate governance
- Demonstration of due diligence in managing risk
- Reduced legal / regulatory vulnerabilities

Bibliography

ISO 31000 : 2009 - Risk Management- Principles and guidelines on implementation.
ISO/IEC 31010: 2009 - Risk management- Risk assessment guidelines
ISO/IEC : 2009 -Guide 73 - Risk Management- Vocabulary

Appendix 1. Defining Risk Criteria

Clause **5.3.5 of ISO31000 reads:**
"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. Risk criteria **should** be consistent with the organization's risk management policy (see 4.3.2), be defined at the beginning of any risk management process and be continually reviewed.

When defining risk criteria, factors to be considered **should** include the following:

- the nature and types of causes and consequences that can occur and how they will be measured;
- how likelihood will be defined;
- the timeframe(s) of the likelihood and/or consequence(s);
- how the level of risk is to be determined;
- the views of stakeholders;
- the level at which risk becomes acceptable or **tolerable;** and
- whether combinations of multiple risks should be taken into account and, if so, how and which combinations should be considered."

Appendix 2. The Meaning of "Reasonably Practicable"

In determining what is (or was at a particular time) reasonably practicable in relation to ensuring health and safety, duty holders must have regard and give appropriate weight to all relevant matters, including:

- **the likelihood** of the hazard or the risk concerned occurring
- the **degree of harm** that might result from the hazard or the risk
- **what the person concerned knows**, or ought reasonably to know, about the hazard or risk, and ways of eliminating or minimising that hazard or the risk
- the **availability and suitability of ways** to eliminate or minimize the hazard or the risk,

and

- the **cost** of eliminating or minimising the hazard or the risk.

<u>What Is 'Reasonably Practicable' Is an Objective Test</u>
What is 'reasonably practicable' is determined objectively. This means that a duty holder

must meet the standard of behaviour expected of a reasonable person in the duty holder's position who is required to comply with the same duty and is:

- committed to providing the highest level of protection for people against risks to their H&S
- proactive in taking measures to protect the health and safety of people.

No single matter determines what is (or was at a particular time) reasonably practicable in relation to ensuring health and safety. The test involves a careful weighing up of each of the matters in the context of the circumstances and facts of the particular case with a clear presumption in favor of safety.

This should be done with regard to the following:

(a) The likelihood of the hazard or the risk concerned occurring

The greater the likelihood of a risk eventuating, the greater the significance this will play when weighing up all matters to be taken into account in determining what is reasonably practicable.

(b) Degree of harm that may result if the hazard or risk eventuated

The greater the degree of harm that could result if the hazard or risk eventuated, the greater the significance this factor will play when weighing up all matters to be taken into account in determining what is reasonably practicable.

(c) What the person concerned knows, or ought reasonably to know, about the hazard or risk and any ways of eliminating or minimising the hazard or risk

Knowledge about the hazard or risk, or any ways of eliminating or minimising the hazard or risk, must be determined objectively by reference to what the duty holder actually knows, and what a reasonable person in the duty-holder's position would reasonably be expected to know.

To comply, a duty-holder must:

- **identify** known occupational hazards within their business or undertaking before they cause an incident, injury or illness (e.g. through a hazard identification process), and
- **understand the nature and degree of harm** that an identified hazard may cause; how the harm can eventuate and the likelihood of that harm occurring. A duty holder may be required to conduct investigations or analyses to gain this understanding (i.e. through a process of risk assessment).

It is also reasonably practicable for a duty-holder to consider and understand within the available state of knowledge how the following impact on hazards and risks:

- potential failure of plant, equipment, systems of work or safety measures
- human error or misuse, spontaneity, panic, fatigue or stress, and
- potential interaction between multiple hazards that may, together, cause different risks.

<u>Reasonable Standard of Knowledge</u>

Duty holders must, as a minimum, know and comply with relevant OHS standards established under the Act, regulations, Codes of Practice and guidelines made under the Act as well as any other relevant legislation.

Other sources of information include:

- reputable technical standards, such as those published by ……
- industry practice and publications, and
- published scientific and technical literature.

(d) Availability / suitability of ways to eliminate / minimize hazards / risks

There are three broad ways of eliminating or minimising risks. These are ranked from most effective and reliable to the least effective and reliable:

1. Eliminate the hazard or risk.
This involves taking action to eliminate a hazard (which eliminates all of its associated risks) or the elimination of the risks associated with the hazard if it cannot be eliminated.

2. If the hazards or risks cannot be eliminated, risks may be minimized by taking action to change the level of risk.
This can involve substituting the risk with a lesser one, engineering measures or changes to systems of work to achieve reductions, or isolating the hazard or risk from people.

3. If hazards or risks cannot be eliminated or minimized, action can be taken to reduce people's exposure to the hazard or risk.
This can involve administrative actions, provision of instruction and procedures, or the use of personal protective equipment.

This ranking is known as the ***hierarchy of control.*** Duty holders are expected to find ways to eliminate or minimize risks in this order. The state of knowledge may provide a number of different ways to control a hazard or risk, and these should be considered when determining what is reasonably practicable in the circumstances. If there are no available or suitable ways to *eliminate* a hazard or risk, then it is necessary to consider all available and suitable ways of *reducing* the risk, so far as is reasonably practicable.

A way of eliminating or minimising a hazard or risk is regarded as suitable if it:

- is feasible to implement in the circumstances
- is effective in eliminating or reducing the likelihood or degree of harm from a hazard or risk
- does not introduce new and higher risks, having regard to all of the circumstances, and
- is a practical measure given the circumstances in which the hazard or risk exists.

For example:

- equipment to eliminate or minimize a hazard or risk is regarded as being available if it is provided on the open market, or if its manufacture is feasible, or
- a work process (or change to a work process) to eliminate or minimize a hazard or risk is regarded as being available if it is feasible to implement.

(e) Cost of eliminating or minimising the hazard or risk
Although the cost of eliminating or minimising a hazard or risk is relevant in determining what is reasonably practicable, there is a clear presumption in favor of safety.

The greater the likelihood of the hazard or risk eventuating, and/or the greater the degree .of harm that would result if the hazard or risk eventuated, the less weight should be given to the cost of eliminating the hazard or risk.

In determining whether a particular level of expenditure is reasonable in the circumstances, the duty-holder must consider:

- the likelihood and degree of harm of the hazard or risk; and
- the reduction of the likelihood and/or
- the reduction of the degree of harm that will result if the safety measure is adopted.

If the degree of harm is significant (e.g. death or serious injury is highly likely) then it is extremely unlikely that the cost of eliminating or reducing the risk would ever be so disproportionate to the risk to justify a decision not to implement an available and suitable safety measure.

Capacity to pay

The question of what is 'reasonably practicable' is to be determined objectively, and not by reference to the duty-holder's capacity to pay or other particular circumstances.

If two duty-holders are faced with the same risk in similar situations, one duty-holder cannot expose people to a lower level of protection simply because it is in a lesser financial position than another duty-holder.

If a particular duty-holder cannot afford to implement a control that is not disproportionate to the risk as to be clearly unreasonable, the duty-holder should not engage in the activity that gives rise to that risk. If there are options available for eliminating or reducing a risk that achieve the same level of reduction in likelihood or degree of harm, a duty-holder may choose the least costly option.

However, choosing a low cost option that provides less protection simply because it is cheaper is unlikely to be considered a reasonably practicable means of eliminating or reducing risk. The costs of implementing a particular control may include costs of purchase, installation, maintenance, operation of the control measure and any impact on productivity as a result of the introduction of the control measure.

A calculation of the costs of implementing a control measure must also take into account savings from fewer incidents, injuries and illnesses, potentially improved productivity and reduced turnover of staff.

Appendix 3. ISO Description of ISO31000

http://www.iso.org/iso/catalogue_detail?csnumber=43170

- ISO 31000:2009 provides principles and generic guidelines on risk management.
- ISO 31000:2009 can be used by any public, private/community enterprise/association, group or individual. Therefore, ISO 31000:2009 is not specific to any industry or sector.
- ISO 31000:2009 can be applied throughout the life of an organization, and to a wide range of activities, including strategies and decisions, operations, processes, functions, projects, products, services and assets.
- ISO 31000:2009 can be applied to any type of risk, whatever its nature, whether having positive or negative consequences.
- Although ISO 31000:2009 provides generic guidelines, it is not intended to promote uniformity of risk management across organizations. The design and implementation of risk management plans and frameworks will need to take into account the varying needs of a specific organization, its particular objectives, context, structure, operations, processes, functions, projects, products, services, or assets and specific practices employed.
- It is intended that ISO 31000:2009 be utilized to harmonize risk management processes in existing and future standards. It provides a common approach in support of standards dealing with specific risks and/or sectors, and does not replace those standards.
- **ISO 31000:2009 is not intended for the purpose of certification.**

Appendix 4. Assigning Risk Owners and Accountability

In the standard, Clause 4.3.3 - Accountability - states clearly that :-
The organization should ensure that there is accountability, authority and appropriate competence for managing risk, including implementing and maintaining the risk management process and ensuring the adequacy, effectiveness and efficiency of any controls. This can be facilitated by:

 identifying **risk owners** that have the accountability and authority to manage risks;

 identifying who is accountable for the development, implementation and maintenance of the framework for managing risk;

 identifying other responsibilities of people at all levels in the organization for the risk management process;

 establishing performance measurement and external and/or internal reporting and escalation processes;

and

 ensuring appropriate levels of recognition.