

Perspective

ISO 31000:2009—Setting a New Standard for Risk Management

Grant Purdy*

Last year saw the publication of ISO 31000:2009, a new globally accepted standard for risk management together with a new, associated vocabulary in ISO Guide 73:2009. These were developed through a consensus-driven process over four years, through seven drafts, and involving the input of hundreds of risk management professionals around the world. The new standard supports a new, simple way of thinking about risk and risk management and is intended to begin the process of resolving the many inconsistencies and ambiguities that exist between many different approaches and definitions. While most decisionmakers seem to welcome the new standard and it has so far received very good reviews, it does create challenges for those who use language and approaches that are unique to their area of work but different from the new standard and guide. The need for compromise and change is the inevitable consequence of standardization

KEY WORDS: ISO 31000; risk management; risk management framework

1. THE PURPOSE OF ISO 31000

While people working in the many different forms of risk management always have the same goal, to provide a sound basis for decisions on whether risks are acceptable and, if necessary, obtain reliable information how they can be dealt with, there are many different definitions of risk and of the risk management process elements and many different versions of the process to be followed. These have all developed for good historical reasons but individuals and organizations, whether they are for profit or not, regulated or regulator, need to make confident and balanced decisions about all risks they have to deal with, on a consistent and reliable basis. Decision-makers are uncomfortable about resolving pieces of apparently similar but fundamentally different information, obtained from different processes and with

different assumptions, that are described using the same words but that have different meanings.

For these reasons, ISO, the international body charged with achieving standardization, set out to achieve consistency and reliability in risk management by creating a standard that would be applicable to all forms of risk. This would contain:

1. One vocabulary;
2. A set of performance criteria;
3. One, common overarching process for identifying, analyzing, evaluating, and treating risks;
4. Guidance on how that process should be integrated into the decision-making processes of any organization.

ISO created a working group comprising experts nominated from 28 countries (up to three from each) and from many other specialist organizations to guide the development of the standard and the associated vocabulary. While the experts possess a very wide range of risk management experience gained in many sectors and applications, their

*Address correspondence to Grant Purdy Broodleaf Capital International Pty Ltd., PO Box 1098, North Mitcham, VIC 3132, Australia; tel: +61 3 9893 0011; purdy@broodleaf.com.au.

principal role has been to represent the views of their respective national and sector mirror committees and organizations.

Through these mirror committees, a network of hundreds of risk management specialists and their customers from around the world have helped create, review, and shape the eventual ISO 31000:2009 and Guide 73. These documents are not therefore just the conclusions of a small committee, but represent the views and experience of hundreds of knowledgeable people involved in all aspects of risk management.

2. WHAT IS RISK?

Standards are not written from the beginning, but from the middle out and it soon became clear to the members of the working group that little real progress could be made with the ISO standard until they all agreed on a definition of risk that arose from a clear and common understanding of what risk is and how it occurs. Dozens of candidate definitions were considered before the working group arrived at:

effect of uncertainty on objectives.

The opening paragraph of the introduction to the standard explains that risk is the consequence of an organization setting and pursuing objectives against an uncertain environment. The uncertainty arises from those internal and external factors and influences that it does not completely control but that may cause the organization to fail to achieve its objectives or may cause delay. These factors and influences can also lead to the objectives being obtained early or exceeded. Risk therefore is neither positive nor negative but the consequences the organization experiences may vary from loss and detriment to gain and benefit.

The ISO 31000 definition of risk shifts emphasis from past preoccupations with the possibility of an event (something happens) to the possibility of an effect and, in particular, an effect on objectives.

When risk is defined like this, it reveals more clearly that managing risk is, quite simply, a process of optimization that makes the achievement of objectives more likely. Risk treatment is then concerned with changing the magnitude and likelihood of consequences, both positive and negative, to achieve a net increase in benefit. Controls then are the outcomes of risk treatment, whose purpose is to modify risk.

It also follows that risks are not events or just consequences. They are descriptions of what could

happen and what it could lead to in terms of how objectives could be affected.

In the past, it has been common for risk to be regarded solely as a negative concept that organizations should try to avoid or transfer to others. However, it is now widely understood that risk is simply a fact of life and is neither inherently good nor inherently bad. To avoid it entirely is to forgo the opportunity of pursuing objectives. If we can successfully detect and understand risk, including how it is caused and influenced, we can, if necessary, change it so that we are more likely to achieve our objectives and might even do this faster, more efficiently, and with improved results.

Risks are either changed or created in all decisions people make: how those decisions are made and the information they are based on will affect whether objectives are achieved in a reasonable time scale. Decision making is, in turn, an integral part of day-to-day existence and nowhere more prominent in an organization than at times of change and when responding to external or internal developments. This is why risk management is an inseparable aspect of managing change and other forms of decision making.

3. THE COMPONENTS OF ISO 31000

3.1. One Vocabulary for Risk Management

It soon became clear to the working group that the definitions of all the terms used in risk management had to be consistent with the underlying processes and vice versa to ensure the guidance in the standard was coherent and practical. For the standard to lead to greater clarity and a wider understanding of risk management, many of the preexisting terms and definitions for process elements that had arisen from different forms of risk and applications of risk management had to change. Fortunately, ISO combined the creation of the standard with a revision of the existing ISO/IEC¹ vocabulary for risk management in Guide 73:2002 and both documents were published at the same time and will be updated together in future.

In that Guide 73 is actually a standard for standards makers and ISO 31000:2009 is a paramount standard, all other ISO and IEC standards that concern themselves with aspects of risk and risk management must now start a process of alignment. Obviously, this process will take some time and the

¹ International Electrotechnical Commission.

compromises needed by those who apply these standards will, in some cases, be quite difficult.

3.2. Performance Criteria

There are some clear performance requirements that, if followed, ensure that risks are managed both effectively and efficiently. The principles of effective risk management in ISO 31000 are that it should:

1. Create and protect value;
2. Be an integral part of all organizational processes;
3. Be part of decision making;
4. Explicitly address uncertainty;
5. Be systematic, structured, and timely;
6. Be based on the best available information;
7. Be tailored;
8. Take into account human and cultural factors;
9. Be transparent and inclusive;
10. Be dynamic, iterative, and responsive to change;
11. Facilitate continual improvement of the organization.

A second list of attributes, in an annex to the standard, contains unavoidable characteristics of managing risk effectively that are also powerful indicators of risk management performance. These include key outcomes, which, while being pretty straightforward, actually describe the ultimate result of effective risk management activity: namely, that the organization will have a current, correct, and comprehensive understanding of its risks and those risks are within its risk criteria. Obviously, if an organization finds on an objective basis that it is not achieving these outcomes, more will need to be done.

The annex also contains the important characteristics of advanced risk management that:

- An emphasis is placed on continual improvement in risk management through the setting of organizational performance goals, measurement, etc.;
- There is comprehensive, fully defined, and fully accepted accountability for risks, controls, and risk treatment tasks;
- All decision making within the organization involves the explicit consideration of risks and the application of risk management to some appropriate degree;
- There is continual communication with external and internal stakeholders, including

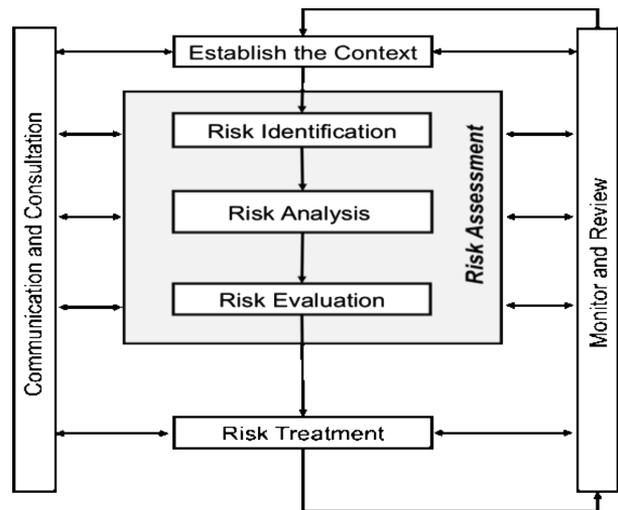


Fig. 1. The risk management process from ISO 31000:2009.

comprehensive and frequent reporting of risk management performance, as part of good governance;

- Risk management is viewed as central to the organization’s management processes, such that risks are considered in terms of effect of uncertainty on objectives.

3.3. The Process for Managing Risk

After considering numerous options and variants, ISO 31000:2009 largely adopted the same broad process as AS/NZS 4360:2004 for managing risk as shown in Fig. 1. While the process is essentially step-like, in practice there is considerably iteration between the steps and between the continuously applied elements of communication and consultation and monitoring and review. Drawing a picture of this is obviously difficult and for this reason, the diagram used in the standard was deliberately not shown as a flow chart. Its purpose is to show the relationship between clauses of the standard that describe the process.

There are two elements of the process that can be considered as continually acting. These are:

- Communication and consultation with internal and external stakeholders, where practicable, to gain their input to the process and their ownership of the outputs. It is also important to understand stakeholders’ objectives, so that their involvement can be planned and

their views can be taken into account in setting risk criteria.

- Monitoring and review, so that appropriate action occurs as new risks emerge and existing risks change as a result of changes in either the organization's objectives or the internal and external environment in which they are pursued. This involves environmental scanning by risk owners, control assurance, taking on board new information that becomes available, and learning lessons about risks and controls from the analysis of successes and failures.

The central spine of the risk management process is concerned with preparing for and then conducting risk assessment leading, as necessary, to risk treatment. The process starts through defining what the organization wants to achieve and the external and internal factors that may influence success in achieving those objectives. This step is called establishing the context and is an essential precursor to risk identification.

Risk assessment under ISO 31000 comprises the three steps of risk identification, risk analysis, and risk evaluation. Risk identification requires the application of a systematic process to understand what could happen, how, when, and why.

In ISO 31000, risk analysis is concerned with developing an understanding of each risk, its consequences, and the likelihood of those consequences. Whether the end result is expressed as a qualitative, semiquantitative, or quantitative manner, gaining this understanding requires consideration of the effect and reliability of existing controls and any control gaps. ISO 31000 does not express a preference for either a quantitative or qualitative approach to risk analysis, as both have a role. Rather, it advises that:

- The way in which consequences and likelihood are expressed and the way in which they are combined to determine a level of risk should reflect the type of risk, the information available, and the purpose for which the risk assessment output is to be used. These should all be consistent with the risk criteria.
- The confidence in determination of the level of risk and its sensitivity to preconditions and assumptions should be considered in the analysis, and communicated effectively to decisionmakers and, as appropriate, other stakeholders.

- Risk analysis can be undertaken with varying degrees of detail, depending on the risk, the purpose of the analysis, and the information, data, and resources available. Analysis can be qualitative, semiquantitative, quantitative, or a combination of these, depending on the circumstances.

Risk evaluation then involves making a decision about the level of risk and the priority for attention through the application of the criteria developed when the context was established.

Risk treatment is the process by which existing controls are improved or new controls are developed and implemented. It involves evaluation of and selection from options, including analysis of costs and benefits and assessment of new risks that might be generated by each option, and then prioritizing and implementing the selected treatment through a planned process. If this process is followed, the systematic way in which the risks have been assessed means that risk treatment can proceed with confidence.

There is a great deal of iteration between risk evaluation and risk treatment as each set of risk treatment options is tested until the preferred set is found that yields the greatest benefit for the least cost.

ISO 31000:2009 gives a set of general options to be considered when risk is treated. The order of the list reflects preference. Importantly, the options deal with both risks that have downside and/or upside consequences. The options are:

- a) Avoiding the risk by deciding not to start or continue with the activity that gives rise to the risk;
- b) Taking or increasing the risk in order to pursue an opportunity;
- c) Removing the risk source;
- d) Changing the likelihood;
- e) Changing the consequences;
- f) Sharing the risk with another party or parties (including contracts and risk financing);
- g) Retaining the risk by informed decision.

3.4. The Framework for Managing Risk

One of the recurrent themes in ISO 31000 is that to be effective, risk management must be integrated into an organization's decision-making processes (which, of course, is how risk is generated). This is easily said but many organizations struggle to achieve this in practice. If the number of pages

indicates some measure of the importance of a subject, then more of the standard (nine pages) is concerned with the implementation of risk management than with the process (seven pages).

Clause 4 of the standard concerns implementation of the risk management process through integration by using a management framework, which consists of the policies, arrangements, and organizational structures to implement, sustain, and improve the process. The standard not only describes the important elements that are required in such a framework but also describes how an organization should go about creating, implementing, and keeping these elements up to date and relevant.

Each organization needs to design or revise the risk management components of its management system to suit its business processes, structure, risk profile, and policies and this is the purpose of a risk management plan. This implementation plan may extend over a considerable time as introducing soundly based risk management usually requires alignment with and even changes to the organization's culture and processes. Large or complex organizations may require a hierarchy of risk management plans but there should always be an overall plan for the organization that describes the broad strategies to be pursued.

The framework described in ISO 31000 can also be adapted and applied to managing risk associated with projects. Although projects often require a different timescale and specialized criteria, they are a source of risk to the organization's objectives and this risk needs to be managed to ensure that projects deliver the value for which they are being undertaken.

4. CONCLUSIONS

Initial drafts of the standard were based on many sources of information. For example, the risk management process came from the Australian and New Zealand Standard, AS/NZS 4360 that, over the last 15 or so years and through three revisions and updates, has become the most widely used standard for risk management in organizations. Also, Clause 4 on implementation through integration was based on an elegant approach, using the organizational improvement cycle of Plan Do Check Act⁽³⁾ in Part 2 in the Austrian standard.⁽⁴⁾ The final version of ISO 31000, however, contains very little of the original text from other standards. It was rewritten, reviewed, and revised so many times that it now seems quite homogeneous and self-supporting.

Of course, despite all the efforts of so many people over such a long timescale, there are always opportunities for improvement and enhancement. The most pressing need, however, is to develop some practical guidance on the implementation of the standard and currently ISO is considering a new work item for that.

Work on revising the standard will start in two years and my views on areas that will need attention then and in preparing guidance now are:

1. The working group quite appropriately avoided getting ensnared in the debate about risk appetite and risk tolerance. These two misused terms reflect confused concepts and poor reasoning that has been sponsored by the ill-founded COSO ERM Framework.⁽⁵⁾ Even a recent review of corporate governance in the financial sector by the Basel Committee on Banking Supervision⁽⁶⁾ says that there is no consensus in that sector on what they mean and the difference between them. ISO 31000 has adopted a more pragmatic approach that requires the organization to derive and set or adopt risk criteria as the basis for its decisions. However, further clear advice is needed to remove all ambiguity about this concept.
2. The working group left unresolved the issue of whether risk treatment should continue until some risk criterion is reached or whether, for even low risks, if it is cost-beneficially desirable, further risk treatment should take place. The former approach arises in health, safety, and environmental legislation, and the latter from business improvement processes. These two approaches are not necessarily inconsistent but could be more smoothly reconciled.
3. The IEC Advisory Committee on Safety (ACOS) removed its support from the working group because it believed that (so-called) safety risks are a special case and should be generally excluded from the generally applied risk management process in ISO 31000. The central argument of ACOS was that any risk to people is unacceptable. The working group did not support this view, as it would lead to most human activities having to cease, so the published standard applies, quite rightly, to all risks whatever the nature of the consequences

that could occur. However, many ISO standards concern safety matters and this difference of opinion must be amicably resolved to ensure consistency and remove any uncertainty.

4. Although the description of the risk management framework in Clause 4 of the standard is quite succinct, nevertheless there remain some elements that could be simplified so that the framework and its implementation become more understandable and appear less onerous for smaller, simpler organizations.

Although there is always room for improvement, the publication of ISO 31000:2009 and Guide 73:2009 represent a very significant milestone in mankind's journey to understand and harness uncertainty. An unprecedented 25 countries voted for the standard with only Italy voting against and, already, it has been formally adopted by many states to replace their national standard and is causing other standard-setting bodies to revisit their documents. As an example, the Institute of Internal Auditors has already published a guide to the planning and execution of risk-based audits and assurance activities using ISO 31000⁽⁷⁾ and is convening a Leadership Summit in August 2010 to help determine its future policy on risk management.

New standards, by their nature, reset goals and ways of thinking and undoubtedly the publication of ISO 31000 now requires all risk management practitioners to examine their current ways of working and the language they use so that their customers, those who are faced with making decisions, obtain simple, consistent, useful, and unambiguous information. Greater consistency in definitions and process can only lead to greater confidence in decision making and, ultimately, to better decisions.

REFERENCES

1. ISO 31000:2009, Risk Management—Principles and Guidelines. Geneva: International Standards Organisation, 2009.
2. ISO Guide 73, Risk Management—Vocabulary. Geneva: International Standards Organisation, 2009.
3. Deming W. *Out of the Crisis*. Cambridge, MA: MIT Center for Advanced Engineering Study, 1986.
4. ONR 49002-2: Risk Management for Organisations and Systems, Part 2 Guidelines for the Integration of Risk Management into the General Management System. Vienna: Austrian Standards Institute, 2004.
5. Enterprise Risk Management—Integrated Framework: Executive Summary. Committee of Sponsoring Organizations of the Treadway Commission, 2004.
6. Basel Committee on Banking Supervision. Consultative Document: Principles for Enhancing Corporate Governance. Basle, Switzerland: Bank for International Settlements, 2010.
7. HB 158, *Delivering Assurance—Based on ISO 31000:2009*. Sydney: Standards Australia and the Institute of Internal Auditors, 2010.