LinkResQ
A LEADER IN ENTERPRISE RISK MANAGEMENT

ISO 31000 Risk Management – Principles and Guidelines

The Why, What and How

A Risk Management White Paper by

Gerard Joyce

LinkResQ Limited

Introduction

In this white paper we review **why** the new ISO 31000:2009 standard is needed, **what** it describes and **how** organisations might go about implementing it.

Why is this standard a good idea?

To help restore investors' and other stakeholders' trust in organisations. Compliance with regulations is no longer enough to secure confidence and trust, organisations must go beyond compliance and demonstrate effective risk management. ISO 31000 will guide organisations in their pursuit of effective risk management. More specifically, the implementation and ongoing maintenance of this standard will enable an organisation to:

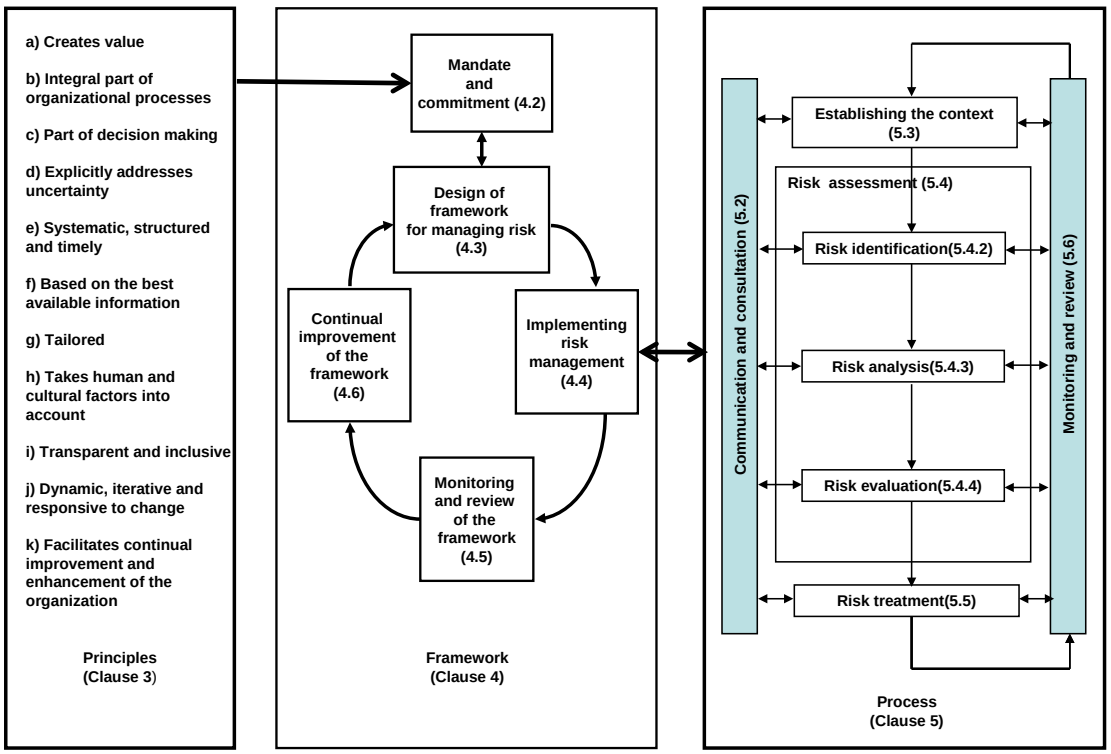
- Increase the likelihood of achieving its objectives
- Improve the identification of opportunities and threats
- Establish a reliable basis for decision making
- Improve organisational effectiveness and efficiency, and
- Improve organisational resilience.

Standards are generally a collation of best practices and when organised in a systematic way they are a blueprint for organisations to deliver consistent processes leading to more efficient and effective operations. ISO 31000 is the culmination of fours years of consultation between hundreds of risk and standards experts in thirty countries. It represents the best source of solid, structured, considered and organised guidelines on the subject of Risk Management.

What exactly is in the standard?

Though this is described as the definitive Risk Management *standard,* its title is more revealing: "Risk management – Principles and guidelines". It clearly states that it is not designed nor intended for certification and the words "must do" do not appear anywhere in the document.

Apart from the introduction and the definition-of-terms-used sections, there are three key clauses in ISO 31000:2009; Principles, Framework and Process. See figure below for how these 3 elements relate to each other.



Source: ISO 3100:2009 Standard

Fig. 1 Relationship between the 3 key clauses of the ISO 31000:2009 standard.

The Principles clause lists eleven principles which should be adhered to if the risk management is to be effective. These include; that risk management is an integral part of all organisational processes, that it is part of decision making, that it is systematic, structured and timely, that it is tailored (to the organisation's context) and that it is dynamic, iterative and responsive to change. If the implementation of risk management is not aligned with these principles then it will be much less effective from an organisational perspective.

The Framework clause describes the management framework required to provide the "foundations and arrangements that will embed it throughout the organisation at all levels." This may sound like another management system, but that is not the intention, rather the structure is the familiar "Plan, Do, Check, Act" methodology and can be readily integrated into existing management systems.

Interestingly, and the figure describing the framework emphasises this, the "mandate and commitment" from the board or senior management must be in place before the cycle of planning, doing, checking and acting can proceed. This is all about the risk management ethos of the organisation and, more than anything else, will determine the success or failure of the risk management programme.

How ISO 31000 is implemented will be largely determined by the nature, scale and complexity of the organisation. The guidelines suggest the evaluation and understanding of "the organisation and its context" before any meaningful planning can begin and offers a comprehensive list of the things that make up the "context". This list includes; the social, cultural, legal, regulatory, financial, technological, natural and competitive environments as well as; policies, objectives, organisational structure, capabilities, standards and contractual relationships.

Risk management policy comes next followed by accountability and resources. These, and how the risk information should be communicated, need to be decided before the implementation can begin. The implementation element is largely what is contained in the "Process" clause (described below).

The guidelines go on to recommend that, as with other aspects of a management system, the risk management framework should be monitored and reviewed to ensure it is working effectively and findings should be fed into decisions that lead to "improvements in the organisation's management of risk."

The Process clause will be familiar to those who have followed the AS/NZS 4360 risk management standard in the past. Its structure is broadly similar. As in the Framework it suggests that the specific context, in which the process is to be implemented, should be established. This will include many of the aspects described in the context under framework, but will also include details pertaining to the scope of the particular risk management process.

Risk criteria (see definition below) need to be defined and aligned with the organisational objectives before any assessment can be carried out. These criteria should include: how likelihood will be defined, how consequences will be measured, how the level of risk is to be determined, and the risk appetite. (see definition below)

The risk assessment process is described under the headings; identification, analysis and evaluation. Specific risk assessment methods are not discussed or prescribed, instead ISO/IEC 31010 is suggested as a guide. Risk analysis is described as the process to "comprehend the nature of the risk and to determine the level of risk". The standard recommends the use of likelihood and consequence(s) (as opposed to impact or severity) to describe the level of risk. "Consequences" is very appropriate here as it conveys breadth, duration and cascading effects of the occurrence of a risk. If the risk criteria are well defined and in particular the risk appetite, then the risk evaluation process – deciding on which risks need treatment and which risks are acceptable – is a relatively straightforward step.

Risk treatment or the "process to modify risk" largely follows the 4 Ts approach; terminate, tolerate, treat or transfer. The "treat" option being to either change the likelihood or change the consequences, the "transfer" option covers insurance, contingency finance and contracts. The standard reminds us that treatment options can in themselves introduce risk and these should also be risk assessed.

As with the framework, each instance of the risk assessment process should be subject to "monitoring and review". This is about ensuring that controls are, and remain, effective and efficient in both design and operation.

Finally the guidelines recommend the recording of risk management activities, as this is fundamental to the ongoing need for continuous improvement of the overall process and a requirement for the compliance with some regulatory obligations.

How does one go about implementing it?

Although ISO 31000 recommends putting an organisation-wide risk management plan in place, it does not prescribe what this plan should look like. Every organisation is different and so every risk management plan will be different. However for those who are looking for a few pointers I would suggest the following for consideration:

- If you are ISO 9001 / 14001 compliant then you will probably already have a template for the creation of a plan.
- Mandate and commitment from the executive team is a pre-requisite for the success of the risk management plan. Put this in place and identify a senior executive who will champion the cause.
- It's good to have dedicated risk officers, but remember that the objective is to **embed** risk management into the organisation. Build it in! Don't just bolt it on!
- Start with the objectives of the organisation. What are you defending? What is lost if you fail to meet your objectives? What matters to your organisation?

If you have the above then you are well on your way to implementing ISO31000:2009.

Many organisations have good instances of risk management within their organisations, but all too often it is neither enterprise-wide nor standardised. ISO 31000 will facilitate the maturing of risk management as a discipline. It will allow all practitioners of risk management (in various functions) to pool their knowledge and expertise and deal in a common currency. You could say that risk management is in the "Norming" phase and with this standard it will finally move into the "Performing" phase and thus progress to full maturity.

Some Definitions. (from ISO Guide 73)

risk - the "*effect of uncertainty on objectives*". This places the emphasis on the effect rather than the event. Think: what consequences could this risk have for the achievement of the objectives?

risk appetite – the "*amount and type of risk that an organisation is prepared to pursue, retain or take*." Difficult to define, but it will make evaluation / treatment decisions a lot easier, while making an organisation's position on risk much more transparent.

risk criteria – "*terms of reference against which the significance of a risk is evaluated*" Some will be dictated by laws and regulations, but most will be determined by the objectives of the organisation and the context in which it operates.

residual risk – "*risk remaining after risk treatment*" This can refer to the collective risk profile after treatment and can contain unidentified risk or it can represent the level of risk still present for a particular risk after controls / treatment of this risk have been taken into account.

risk owner – "*person or entity with the accountability and authority to manage the risk*" Risk owners need to be empowered to implement changes / controls to manage the risk.

likelihood – "*chance of something happening*" This can be described qualitatively, quantitatively or semi-quantitatively.

consequence – "outcome of an event affecting objectives" Can be positive or negative. Initial consequences can escalate through knock-on effects.

Gerard Joyce is a director of LinkResQ @linkresq.ie, a member of the Institute of Risk Management, chairman of the Irish consultative committee on risk management and member of the ISO TMB Risk Management Working Group.

LinkResQ Ltd, 4200 Atlantic Avenue, Westpark, Shannon Co. Clare, Ireland
Tel: + 353-61-477 888, email: @linkresq.ie web: .linkresq.ie

