ISO 31000:2009 A FRAMEWORK FOR MANAGING YOUR BUSINESS

The International Organisation for Standardisation (ISO) produced ISO 31000:2009 Risk management – Principles and guidelines as a guidance standard for risk management. It is a generic standard, intended for use by any type or size of organisation.

The standard provides an holistic approach to the implementation of effective risk management arrangements. Usefully this approach is presented within the well-established ISO continual improvement structure of Plan, Do, Check, Act.

As a basis for effective risk management the standard sets out eleven Principles which should be applied at all levels. These include: “Risk management creates and protects value”, “Risk management is part of decision making” and “Risk management is dynamic, iterative and responsive to change”. These principles are defined and explained and a further appendix is provided for guidance.

a flexible framework for better business

BASED ON THE PLAN DO CHECK ACT CYCLE IT DRIVES CONTINUOUS IMPROVEMENT IN RISK MANAGEMENT

The framework set out in the standard is made up of the following stages:

- establishing the mandate and commitment to risk management
- designing the framework for managing risk and establishing a risk management policy
- integration of risk management into organisational processes
- allocation of appropriate resources
- establishing internal and external communication and reporting mechanisms
- implementing the framework and a risk management process,
- monitoring and review of the framework
- continual improvement of the framework
PROCESS

The main elements of the process outlined in the standard are recognisably part of the traditional risk management process: risk identification, analysis, evaluation and treatment.

RISK CRITERIA

This is defined as “the terms of reference against which the significance of a risk is evaluated”. Criteria help in deciding the significance of a risk based upon its possible effects and likelihoods. Typical considerations guided by the criteria would be considerations of the benefit of reducing risk level compared with the cost increasing controls. Criteria should also state the consequences to be considered as part of risk assessment – including loss of life, financial loss and reputation impact. Again an understanding of the organisation’s context will help in defining appropriate criteria.

ENTERPRISE RISK MANAGEMENT

One of the key features of the standard is the level of significance it gives to gaining a proper understanding the organisation's internal and external contexts. This understanding should be one of the main drivers for the design of both the risk management framework and process. Such an approach will help to ensure a “best fit” for the organisation’s risk management needs.

RISK TREATMENT

This is the “the process to modify risk” and is an organization’s response to a given risk. Responses could include avoiding the risk, taking or increasing the risk, changing its likelihood and / or consequences or sharing the risk.

Underpinning the process – and diagrammatically presented as being linked to all of the process stages – are the two fundamental concepts of:

- Communication and consultation
- Monitoring and review

In terms of both the framework and process, if an organization properly evaluates and understands its internal and external contexts then this will provide a robust basis for the design, implementation and operation of its risk management arrangements.
ISO are clear on the benefits of applying the standard: “Risks affecting organisations can have consequences in terms of economic performance and professional reputation, as well as environmental, safety and societal outcomes. Therefore, managing risk effectively helps organisations to perform well in an environment full of uncertainty.” Implementing effective risk management arrangements bring an array of specific benefits to an organisation. These include:

- Minimising losses, improving resilience and better governance
- Compliance with legal and regulatory requirements
- Improved stakeholder confidence and trust

So, in summary, organisations can improve their overall reputation and brand standing, increase the likelihood of achieving objectives, improve the identification of opportunities and threats and allocate and use resources for risk treatment effectively.

Risk management becomes a key driver of success and an integral part of core business activities such as strategic and operational planning, management decision-taking and governance.