White Paper on ISO 31000

RISK MANAGEMENT

Sterling

INTRODUCTION

Risk management is an increasingly important business driver and stakeholders have become much more concerned about risk. Risk may be a driver of strategic decisions, it may be a cause of uncertainty in the organization or it may simply be embedded in the activities of the organization.

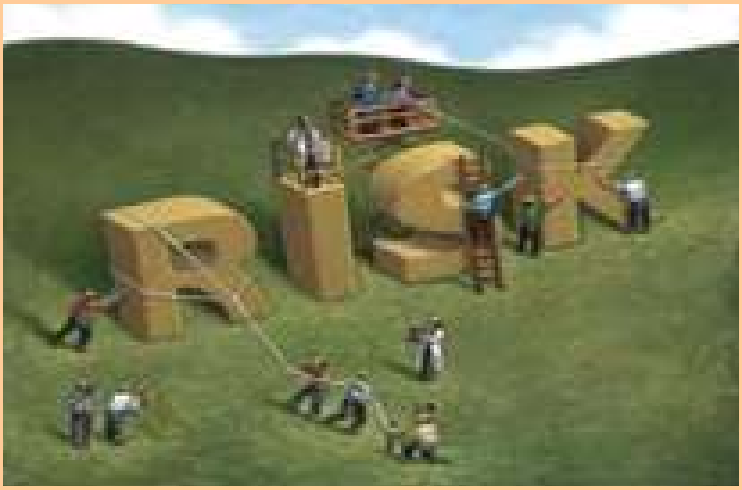
An enterprise-wide approach to risk management enables an organization to consider the potential impact of all types of risks on all processes, activities, stakeholders, products and services. Implementing a comprehensive approach will result in an organization benefiting from what is often referred to as the 'upside of risk'

ISO 31000:2009 provides generic guidelines for the design, implementation and maintenance of risk management processes throughout an organization.

It is a framework that can be integrated across various industries and regions and adopted by any organization – including public, private, not-for-profit and government organizations.

The scope of this approach to risk management is to enable all strategic, management and operational tasks of an organization throughout projects, functions, and processes to be aligned to a common set of risk management objectives.

ISO 31000 was published as a standard on the 13th of November 2009, and provides a standard on the implementation of risk management. The purpose of ISO 31000:2009 is to be applicable and adaptable for "any public, private or community enterprise, association, group or individual. Accordingly, the general scope of ISO 31000 - as a family of risk management standards - is not developed for a particular industry group, management system or subject matter field in mind, rather to provide best practice structure and guidance to all operations concerned with risk management.



APPLICATION OF ISO 31000

ISO 31000:2009 provides generic guidelines for the design, implementation and maintenance of risk management processes throughout an organization. This approach to formalizing risk management practices will facilitate broader adoption by companies who require an enterprise risk management standard that accommodates multiple 'silo-centric' management systems.

Accordingly, ISO 31000:2009 is intended for a broad stakeholder group including:

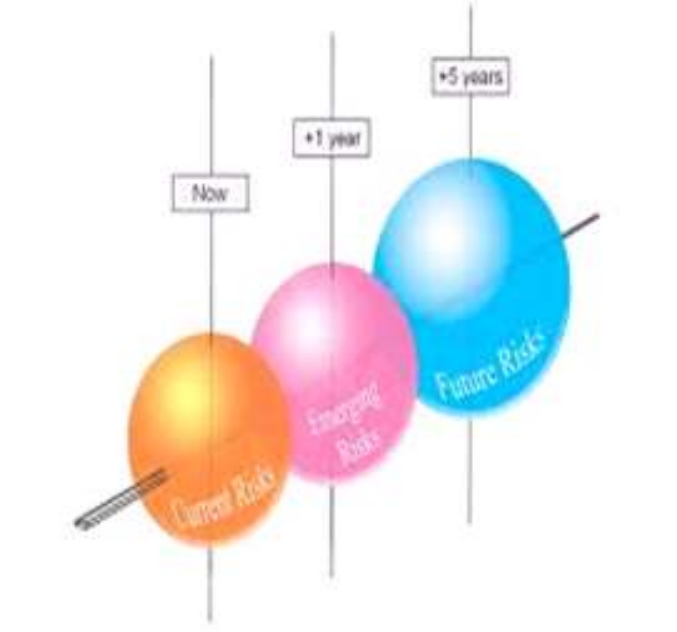
- executive level stakeholders
- appointment holders in the enterprise risk management group
- risk analysts and management officers
- line managers and project managers
- compliance and internal auditors
- Independent Practitioners

BENEFITS OF ISO 31000 – RISK MANAGEMENT

For all types of organizations, there is a need to understand the risks being taken when seeking to achieve objectives and attain the desired level of reward. Organizations need to understand the overall level of risk embedded within their processes and activities. It is important for organizations to recognize and prioritize significant risks and identify the weakest critical controls.

When setting out to improve risk management performance, the expected benefits of the risk management initiative should be established in advance. The outputs from successful risk management include compliance, assurance and enhanced decision-making. These outputs will provide benefits by way of improvements in the efficiency of operations, effectiveness of tactics (change projects) and the efficacy of the strategy of the organization.

A successful risk management initiative can affect the likelihood and consequences of risks materializing, as well as deliver benefits related to better informed strategic decisions, successful delivery of change and increased operational efficiency.



Other benefits include reduced cost of capital, more accurate financial reporting, competitive advantage, improved perception of the organization, better marketplace presence and, in the case of public service organizations, enhanced political and community support.

Risk management is a process which provides assurance that:

- objectives are more likely to be achieved;
- damaging things will not happen or are less likely to happen;

beneficially things will be or are more likely to be achieved.

It is avoiding risk. The aim of risk management is not to eliminate risk, rather to manage the risks involved in all activities to maximise opportunities and minimise adverse effects.

Good risk management provides upward assurance from business activities and administrative functions, from department to faculties, to the senior management team and ultimately to the governing body.

The potential benefits from risk management are:

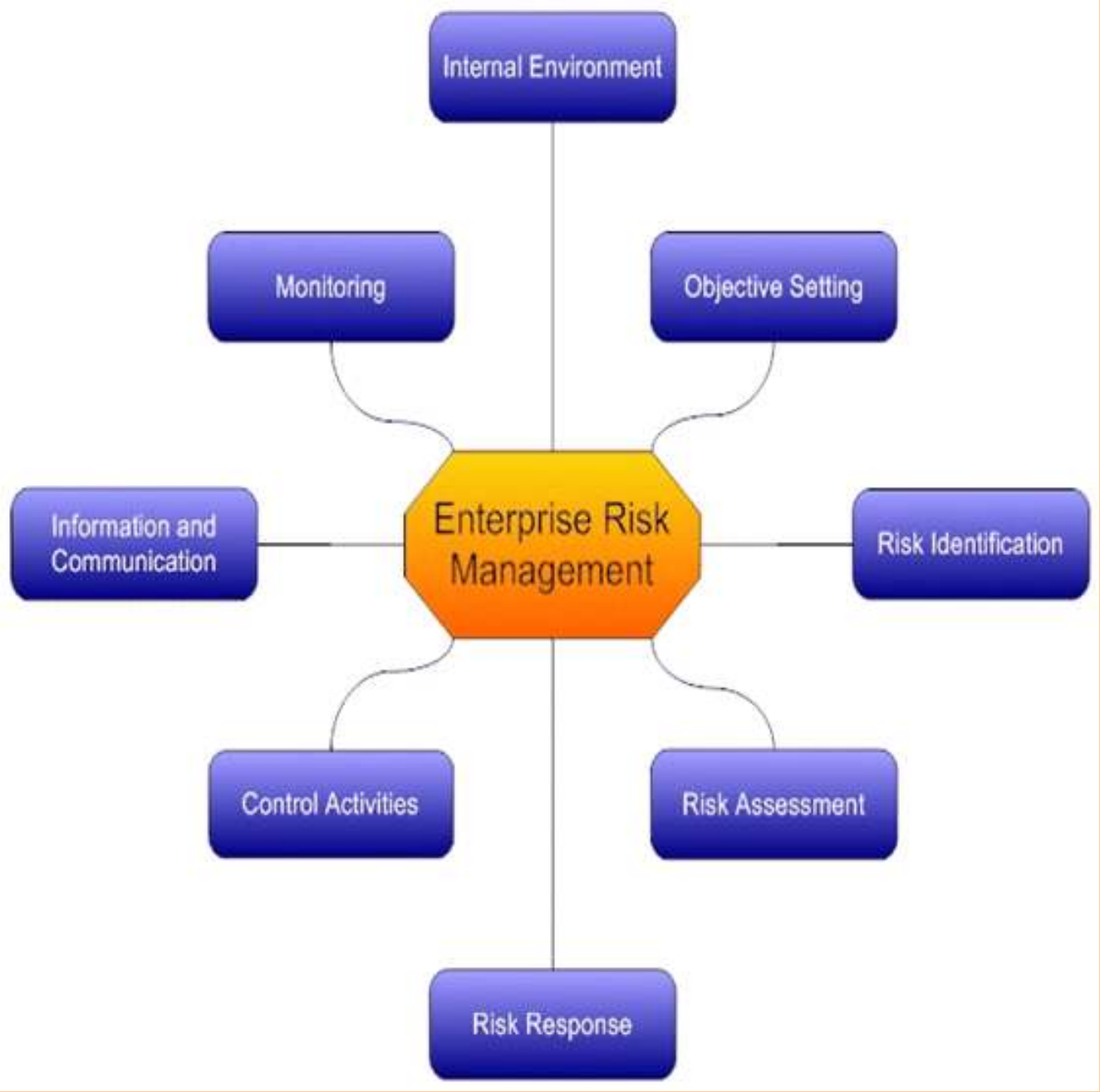
- supporting strategic and business planning;
- supporting effective use of resources;
- promoting continuous improvement;
- fewer shocks and unwelcome surprises;
- quick grasp of new opportunities;
- enhancing communication between Organisations and Departments;
- reassuring stakeholders;
- helping focus internal audit programme;

Sterling International Consulting:- 202, Gym Building, Khalid Bin Waleed Street, Bur Dubai, PO BOX 27363, Dubai, UAE
Phone: +971 4455 8677, Mobile: +971 5058 42597 | Fax: +971 4455 8556 Web: www.uaeiso.com | Email: info@uaeiso.com
• U.S.A • UK • SINGAPORE • INDIA • UAE • KSA • EUROPE • AFRICA • AUSTRALIA • HONG KONG

ELEVEN PRINCIPLES OF RISK MANAGEMENT

Risk management is a process that is under-pinned by a set of principles. Also, it needs to be supported by a structure that is appropriate to the organization and its external environment or context. A successful risk management initiative should be proportionate to the level of risk in the organization (as related to the size, nature and complexity of the organization), aligned with other corporate activities, comprehensive in its scope, embedded into routine activities and dynamic by being responsive to changing circumstances.

This approach will enable a risk management initiative to deliver outputs, including compliance with applicable governance requirements, assurance to stakeholders regarding the management of risk and improved decision-making. The impact or benefits associated with these outputs include more efficient operations, effective tactics and efficacious strategy. These benefits need to be measurable and sustainable.



1. Creates and protects value

Good risk management contributes to the achievement of an agency's objectives through the continuous review of its processes and systems.

2. Be an integral part of organizational processes

Risk management needs to be integrated with an agency's governance framework and become a part of its planning processes, at both the operational and strategic level.

3. Be part of decision making

The process of risk management assists decision makers to make informed choices, identify priorities and select the most appropriate action.

4. Explicitly address uncertainty

By identifying potential risks, agencies can implement controls and treatments to maximise the chance of gain while minimizing the chance of loss.

5. Be systematic, structured and timely

The process of risk management should be consistent across an agency to ensure efficiency,consistency and the reliability of results.

6. Based on the best available information

To effectively manage risk it is important to understand and consider all available information relevant to an activity and to be aware that there may be limitations on that information. It is then important to understand how all this information informs the risk management process.

7. Be tailored

An agency's risk management framework needs to include its risk profile, as well as take into consideration its internal and external operating environment.

8. Take into account human and cultural factors

Risk management needs to recognize the contribution that people and culture have on achieving an agency's objectives.

9. Be transparent and inclusive

Engaging stakeholders, both internal and external, throughout the risk management process recognizes that communication and consultation is key to identifying, analyzing and monitoring risk.

10. Be dynamic, iterative and responsive to change

The process of managing risk needs to be flexible. The challenging environment we operate in requires agencies to consider the context for managing risk as well as continuing to identify new risks that emerge, and make allowances for those risks that no longer exist.

11. Facilitate the continual improvement of organizations

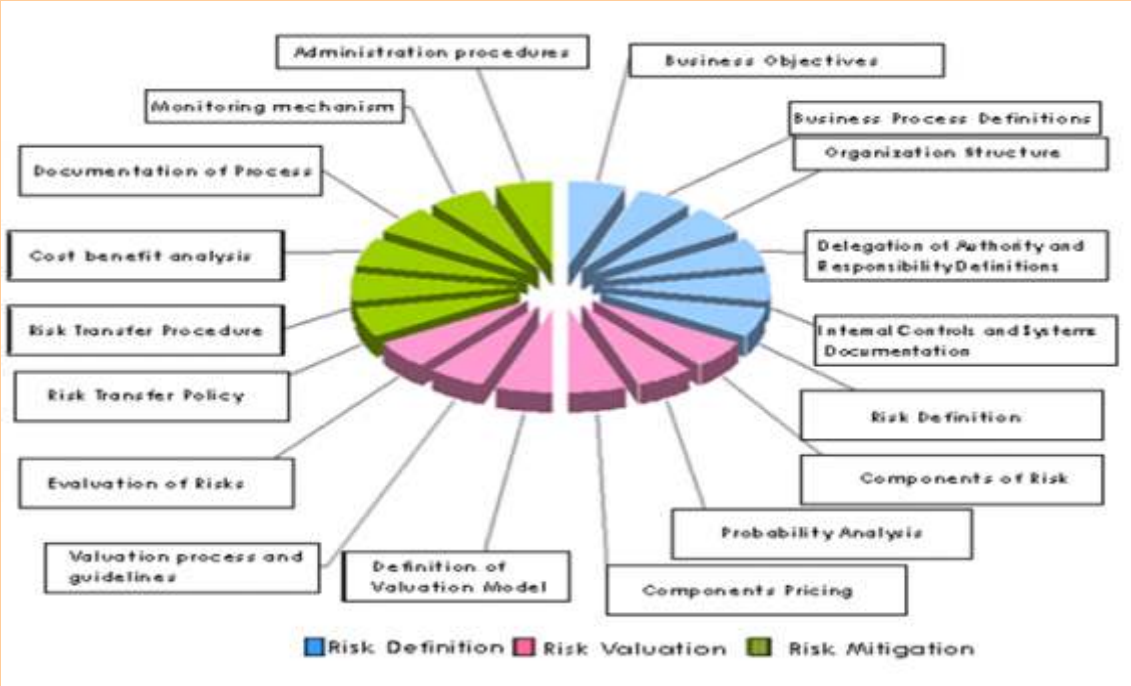
Agencies with a mature risk management culture are those that have invested resources over time and are able to demonstrate the continual achievement of their objectives.

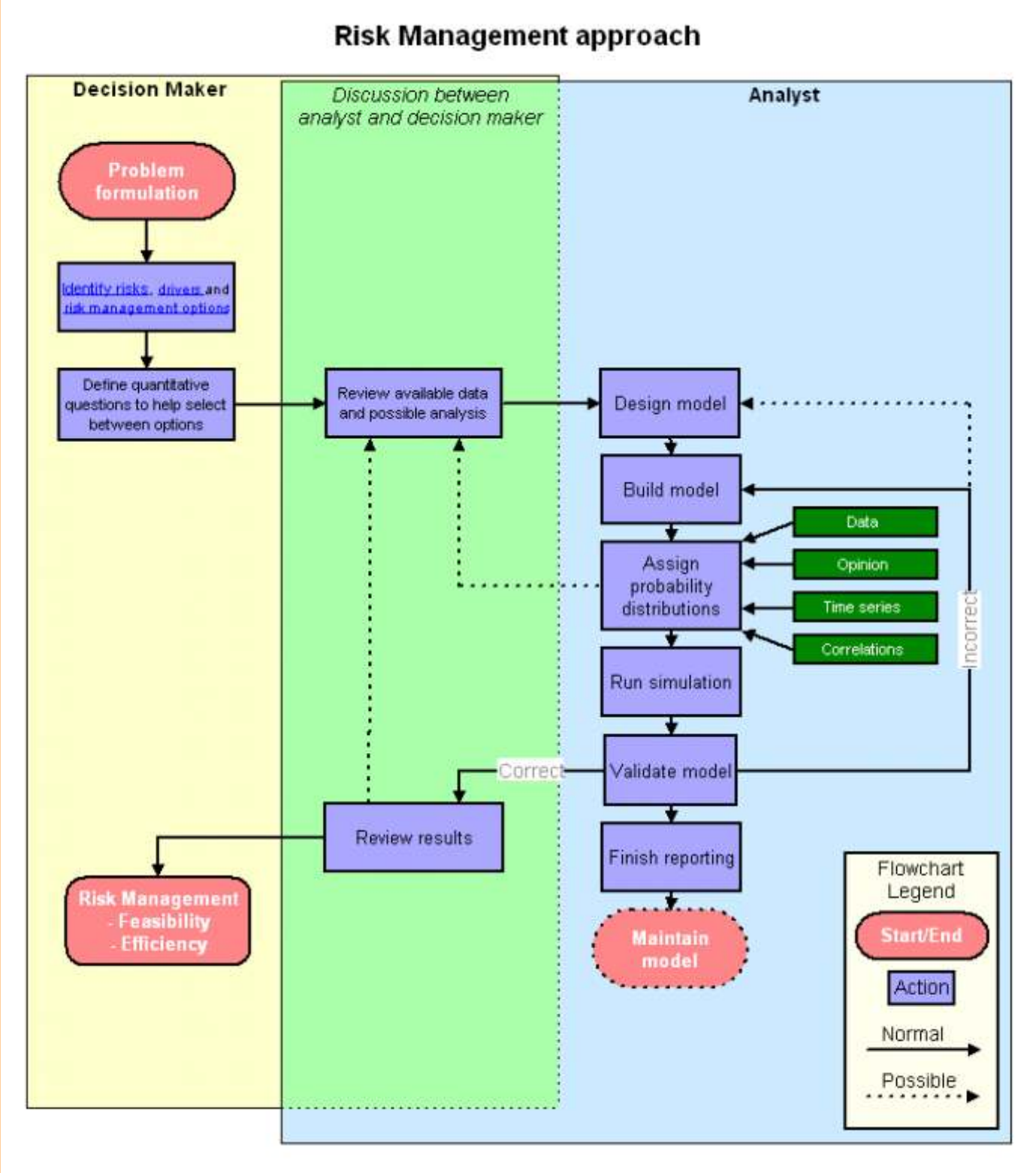
5 Attributes to Enhance Risk Management.

Enhanced risk management should have five attributes;

- Emphasis on continuous improvement through setting organizational performance goals, measurement, review, and modification of processes, systems, resources, capability and skills.
- Comprehensive, defined and accepted accountability for risks, controls and treatment tasks. Identified individuals accept, are appropriately skilled, and have adequate resources to check controls, monitor risks, improve controls and communicate about risks and management to interested parties.
- Decisions at all levels explicitly consider risks and application of the risk management process.
- Continual communication, visible, comprehensive and frequent reporting of risk management performance to interested parties as part of a governance process.

Viewed as a core organizational process, considering sources of uncertainty that could be treated to maximize the chance of gain and minimize the chance of loss. Regarded by senior managers as essential for achieving organizational objectives. Governance structure and process must be founded on a risk management process.




Risk Management approach
Decision Maker
Discussion between analyst and decision maker
Analyst
Problem formulation
Identify risks, drivers and risk management options
Define quantitative questions to help select between options
Review available data and possible analysis
Design model
Build model
Data
Opinion
Time series
Correlations
Assign probability distributions
Run simulation
Validate model
Incorrect
Correct
Review results
Finish reporting
Risk Management
- Feasibility
- Efficiency
Maintain model
Flowchart Legend
Start/End
Action
Normal
Possible

RISK ASSESSMENT

Risk assessment involves the identification of risks followed by their evaluation or ranking. It is important to have a template for recording appropriate information about each risk. A simple description of a risk is sufficient, but sometimes there are circumstances where a detailed risk description may be required in order to facilitate a comprehensive risk assessment process.

The consequences of a risk materialising may be negative (hazard risks), positive (opportunity risks) or may result in greater uncertainty. Organisations need to establish appropriate definitions for the different levels of likelihood and consequences associated with these different risks. Risk ranking can be quantitative, semi-quantitative or qualitative in terms of the likelihood of occurrence and the possible consequences or impact.

An important part of analysing a risk is to determine the nature, source or type of impact of the risk. Evaluation of risks in this way may be enhanced by the use of a risk classification system. Risk classification systems are important because they enable an organisation to identify accumulations of similar risks. A risk classification system will also enable an organisation to identify which strategies, tactics and operations are most vulnerable.

Risk classification systems are usually based on the division of risks into those related to financial control, operational efficiency, reputational exposure and commercial activities.

Risk management should be a continuous process that supports the development andimplementation of the strategy of an organisation.

It should methodically address all the risks associated with all of the activities of the organisation. In all types of undertaking, there is the potential for events that constitute opportunities for benefit (upside), threats to success (downside) or an increased degree of uncertainty.

RISK MANAGEMENT PROCESS

The risk management process can be presented as a list of co-ordinated activities. There are alternative descriptions of this process, but the components listed below are usually present. This list represents the 7Rs and 4Ts of (hazard) risk management:

- recognition or identification of risks
- ranking or evaluation of risks
- responding to significant risks
    - tolerate
    - treat
    - transfer
    - terminate
- resourcing controls
- reaction planning
- reporting and monitoring risk performance
- reviewing the risk management
- framework

Recognition and ranking of risks together form the risk assessment activity. ISO 31000 uses the phrase 'risk treatment' to include all of the 4Ts included under the heading 'risk response'. The scope of risk responses available for hazard risks includes the options of tolerate, treat, transfer or terminate the risk or the activity that gives rise to the risk. For many risks, these responses may be applied in combination. For opportunity risks, the range of available options includes exploiting the risk. Reaction planning includes business continuity planning and disaster recovery planning.

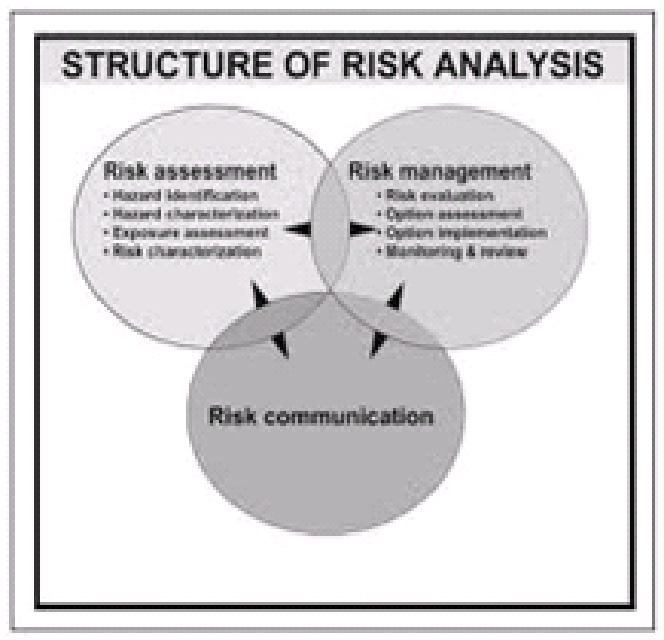
FRAMEWORK FOR MANAGING RISK

ISO 31000 describes a framework for implementing risk management, rather than a framework for supporting the risk management process. Information on designing the framework that supports the risk management process is not set out in detail in ISO 31000. An organisation will describe its framework for supporting risk management by way of the risk architecture,strategy and protocols for the organisation.

It also sets out the roles and responsibilities of the individuals and committees that support the risk management process. The risk strategy should set out the objectives that risk management activities in the organisation are seeking to achieve.

RISK TREATMENT

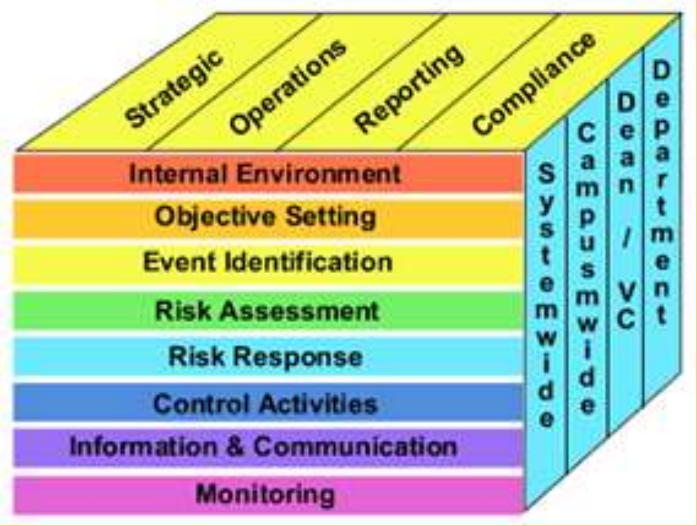
Risk treatment is presented in ISO 31000 as theactivity of selecting and implementing appropriatecontrol measures to modify the risk. Risktreatment includes as its major element, riskcontrol (or mitigation), but extends further to, forexample, risk avoidance, risk transfer and riskfinancing. Any system of risk treatment shouldprovide efficient and effective internal controls.Effectiveness of internal control is the degree towhich the risk will either be eliminated or reducedby the proposed control measures. The cost effectivenessof internal control relates to the costof implementing the control compared to the riskreduction benefits achieved.



Compliance with laws and regulations is not anoption. An organisation must understand theapplicable laws and must implement a system ofcontrols that achieves compliance.

FEEDBACK MECHANISMS

ISO 31000 recognizes the importance of feedback by way of two mechanisms. These are monitoring and review of performance and communication and consultation. Monitoring and review ensures that the organisation monitors risk performance and learns from experience. Communication and consultation is presented in ISO 31000 as part of the risk management process, but it may also beconsidered to be part of the supporting framework.



STEPS INVOLVED IN IMPLEMENTATION OF RISK MANAGEMENT

PLANNING AND DESIGNING

There are a number of factors that should beconsidered when designing and planning an ERM initiative. Details of the risk architecture, strategyand protocols should be recorded in a risk management policy for the organisation.

A risk management policy ensures that the overall risk management approach is in line with current best practice. It also gives the organisation the opportunity to focus on the intended benefits for the coming year, identify the risk priorities and ensure that appropriate attention is paid to emerging risks. The policy should also describe the risk architecture of the organisation.

Mandatory commitment from the Board is critically important and it needs to be continuous. Unless the commitment is not forthcoming, the risk management initiative will be unsuccessful. Keeping the risk management policy up to date demonstrates that risk management is a dynamic activity fully supported by the Board.

IMPLEMENTATION

Risk assessment is a fundamentally important part of the risk management process. In order to achieve a comprehensive risk management approach, an organisation needs to undertake suitable and sufficient risk assessments.

An organisation should develop benchmarks to determine the significance (or materiality) of the identified risks. The nature of these benchmark tests will depend on the type of risk.

Other considerations relevant to undertaking risk assessments include decisions on how the risk assessments will be recorded, the level of detail that will be recorded about each risk in the risk description. Another important part of the risk assessment will be the identification of the risk classification system to be used by the organisation.

Risk assessment of all proposed activities should be undertaken and further risk assessments should be undertaken.

MEASURING AND MONITORING

Observations from the risk assessments are recorded in a risk register. The risk register should not become a static record of the significant risks faced by the organisation. It should be viewed as a risk action plan that includes details of the current controls and details of any further actions that are planned.

These further actions should be written as auditable actions that must be completed within a defined timescale by identified individuals. This will enable the internal audit function to monitor the existing controls and monitor the implementation of any necessary additional controls. The resources required to implement the risk management policy should be clearly established at each level of management and within each business unit. Risk management should be embedded within the strategic planning and budget processes as well as monitoring the effectiveness of the existing controls and the implementation of additional controls, the cost-effectiveness of the existing controls should also be monitored.

Additionally, monitoring and measuring includes evaluation of the risk aware culture and the risk management framework, and assessment of the extent to which risk management tasks are aligned with other corporate activities.

EVALUATE EXISTING CONTROLS

Monitoring and measuring extends to the evaluation of culture, performance and preparedness of the organisation. The scope of activities covered by monitoring and measuring also includes monitoring of risk improvement recommendations and evaluation of the embedding of risk management activities in the organisation, as well as routine monitoring of risk performance indicators.

Monitoring the preparedness of the organisation tocope with major disruption is an important part of risk management. This activity normally extends to the development and testing of business continuity plans and disaster recovery plans. There is a need to keep these plans up to date so that the preparedness of the organisation to cope with the identified risk events is assured.

Evaluation of the existing controls will lead to the identification of risk improvement recommendations. These recommendations should be recorded in the risk register by way of a risk action plan. An important part of evaluating the effectiveness of existing controls is to ensure that there is adequate evaluation of the business continuity planning and disaster recovery planning arrangements in place.

REPORT RISK PERFORMANCE

In addition to internal communication and reporting, there is an obligation on theorganisations to report externally. External risk reporting isdesigned to provide external stakeholders with assurance that risks have been adequately managed.

External reporting provides useful informationto stakeholders on the status of risk management and the actions that are being taken to ensure continuous improvement in performance. A company needs to report to its stakeholders on a regular basis, setting out its risk management policies and the effectiveness in achieving its objectives. Increasingly, stakeholders look to organisations to provide evidence of appropriate corporate behaviour in such areas as community affairs, human rights, employment practices, health and safety, and the environment.

Risk reporting provides information on historical. Important lessons can be learned that will assist with improving the design of the support framework and the implementation framework.

CERTIFICATION

Once the Risk Management System is in place and the organization is confident of having met all the requirements, the external audit and certification process can be initiated. This process requires multiple steps:

A site visit is conducted by the certification body to audit the company with respect to the requirements of the standard. The audit includes interview, inspections of facilities and records.

The time requirement for a small company is as little as one day. Larger organizations canexpect the audit to be conducted within several days.

After the site visit, an audit report will be submitted to top-management including the results and recommendations for improvements.

The last step is the issue of the certificate. The certificate is valid for three years. After conducting the first audit and the certificate is issued, the certification body will conduct surveillance audits on a regular basis(yearly follow-ups).

WHAT WE OFFER?

With a team of highly qualified consultants and trainers having vast industrial experience, Sterling International Consulting. partners organizations across the world to implement and achieve ISO 31000certification.

Our consulting approach is highly professional, time bound and effective resulting in ease of implementation and adds value to the business processes of the client organization.

Contact us at info@uaeiso.com to
get your organization ISO 31000 certified.

Sterling International Consulting:- 202, Gym Building, Khalid Bin Waleed Street, Bur Dubai, PO BOX 27363, Dubai, UAE

Phone: +971 4455 8677, Mobile: +971 5058 42597 | Fax: +971 4455 8556 Web: www.uaeiso.com | Email: info@uaeiso.com

24 Hours
customer Care
+971 5058 42597

White Paper on ISO 31000
RISK MANAGEMENT

STERLING INTERNATIONAL CONSULTING
202, Gym Building, Khalid Bin Waleed Street,
Bur Dubai, PO BOX 27363, Dubai, UAE
Phone: +971 4455 8677, Mobile: +971 56201 4736
Fax: +971 4455 8556 • Web: www.uaeiso.com
Email: info@uaeiso.com