**The Gold Standard for Risk Management – ISO 31000/ASNI Z-690**

By Jim Newberry

**What Risk Management and Risk Assessment mean for Safety Profession**

Risk management and risk assessment are ways to gain access to upper levels of management to show them what you can do for them in language they understand.

* + Safety becomes one of the action areas that helps implement programs profitably
	+ Risk is a concept upper management understands and uses regularly in all areas of corporate operations and planning

**INTRODUCTION**

This risk management guideline provides organizations of all types with a well-stocked toolbox for tackling situations that could affect the achievement of their objectives.  Risks affecting organizations may have consequences in terms of: a) societal, b) environmental, c) technological, d) safety, e) security outcomes, f) commercial, g) financial and economic disciplines, h) social, i) cultural and political as well as j) reputation impacts. When risks arise, organizations always have to ask the question: "Is the level of risk acceptable, and does it require consideration for further action?"

Risk assessment is an integral part of risk management which provides a structured process for organizations to identify how objectives may be affected. Risk assessment tools are used to analyze risks in terms of consequences and their probabilities, before the organization decides on further treatment, if required. Risk assessment provides decision-makers and responsible parties with an improved understanding of risks that could affect achievement of objectives, as well as, of the adequacy and effectiveness of controls already in place. The ISO 31010 guidelines provide a basis for decision about the most appropriate approach to be used to treat particular risks and to select between options.

**CHARACTERISING RISK**

We characterize and describe risk in terms of both consequence and what could happen and the likelihood of those consequences. In the past some standards only described risks as sudden or accidental events. However, we can now appreciate that risk also arise because of slowly changing or chronic situation and circumstances, not just because of a sudden event. Climate change is an example of a changing situation that poses a great risk to organizations, and indeed to the planet, yet it is not a single event.

There are challenges in characterizing both consequence and likelihoods. One simple way of describing potential consequences is to say what could happen and what could it lead to. The consequences we use to describe risk may involve loss, harm, and detrimental effects but often they involve benefits and advantages as well. In many cases, whether we describe consequences in a negative or positive frame depends on our point of view. For example, sometimes our loss will be someone else's gain. This positive framing of risk is becoming more commonly referred to as “opportunity risk” and it is to our benefit to expand our point of view to incorporate this larger view of risk

Importantly and fundamentally, risk is characterized and measured by considering consequences and likelihood of those consequences, not the abstract likelihoods of events that might be detached from your organizations objectives. Consequences and their likelihoods are combined in this framework to define a level of risk that quantifies it and to determine if treatment is required.

**THE PRINCIPLES OF RISK MANAGEMEMT**

1. **Risk Management should create and protect value.**
* **Create and protect value by using risk management to help achieve your organization’s objectives and improve its performance.**
1. **Risk Management should be an integral part of all processes**
* **Make risk management part of every process within your organization at every level.**
* **Make risk management a responsibility of every manager within your organization.**
1. **Risk Management should be a part of your decision making process at every level.**
* **Use risk management to make informed choices.**
* **Use risk management to prioritize actions.**
1. **Risk Management should be used to address the uncertainty that your organization faces.**
* **Use risk management to identify and define the nature and type of uncertainties that your organization must deal with.**
* **Use risk management to figure out what you can do to address your organization’s uncertainties.**
1. **Risk Management should use an approach that is structured, systematic, and timely.**
* **Make sure that your approach contributes to organizational efficiency.**
* **Make sure that your approach generates consistent and reliable results.**
1. **Risk Management should be based on the best information available.**
* **Make sure that the inputs you use to manage risk are based on the best available information sources.**
* **Make sure that decision makers understand and consider the limitations and shortcomings of the data they use to manage risk.**
1. **Risk Management should be tailored to your environment.**
* **Make sure that your organization’s approach to risk management is aligned with its unique internal and external context.**
* **Make sure that your organization’s approach to risk management is aligned with its risk profile.**
1. **Risk Management should consider both human and cultural factors**
* **Make sure that your approach to risk management recognizes and considers the human and cultural factors that can influence the achievement of your organization’s objectives.**
* **Consider how human capabilities can facilitate or hinder the achievement of your objectives.**
* **Consider how human perceptions can facilitate or hinder the achievement of your objectives.**
* **Consider how human intentions can facilitate or hinder the achievement of your objectives.**
1. **Risk Management should be transparent, inclusive and relevant**
* **Make sure that your organization’s approach to risk management is open, visible, and accessible.**
* **Involve your organization’s stakeholders.**
* **Involve decision makers from all parts of your organization.**
1. **Risk Management practices should be dynamic and responsive.**
* **Make sure that your approach to risk management continually senses change and responds to it.**
* **Make sure that your organization’s approach to risk management is iterative (a process that repeats itself).**
* **Repeat your risk management process whenever and wherever objectives need to be achieved.**
1. **Risk Management should facilitate continual improvement**
* **Use risk management to continually improve all aspects of your organization.**
* **Develop strategies to continually improve your approach to risk management.**

**THE RISK MANAGEMENT FRAMEWORK**

1. **Make risk management part of your organization’s management system.**
* **Establish an effective risk management framework for your organization.**
* **Use your framework to support your organization’s management process.**
1. Make a commitment to Risk Management
* Define your organization’s risk management policy.
* Establish risk management performance indicators.
* **Formulate risk management objectives.**
* **Assign risk management responsibilities.**
* **Allocate risk management resources.**
* **Communicate risk management benefits.**
* **Support your risk management framework.**
1. **Evaluate and understand your organization’s internal and external context and then use this knowledge to help design your risk management framework.**
* **Evaluate and understand your organization’s external environment.**
* **Evaluate and understand your organization’s external stakeholders.**
* **Evaluate and understand your organization’s external influences.**
* **Evaluate and understand your organization’s internal context and then use this knowledge to help design your risk management framework.**
* **Understand your organization’s internal stakeholders.**
* **Understand your organization’s governance.**
* **Understand your organization’s capabilities.**
* **Understand your organization’s culture.**
* **Understand your organization’s standards.**
* **Understand your organization’s contracts.**
1. Formulate your Risk management policy
* **Establish a risk management policy for your organization.**
* **Make a clear commitment to risk management.**
* **Define your risk management objectives.**
* **Explain how your policy will be implemented.**
* Communicate your risk management policy.
1. Make people accountable for managing risk
* Identify your organization’s risk owners.
* Give risk owners the authority to manage risk.
* **Make risk owners accountable for managing risk.**
* **Establish risk management performance measurement methods.**
* **Develop risk management reporting and escalation processes.**
1. Build Risk Management into your organization
* **Make risk management an integral part of all processes and practices.**
* **Develop an organization-wide risk management plan.**
1. **Allocate appropriate resources to support your organization’s risk management activities.**
* **Consider providing people who can support your organization’s risk management activities.**
* **Consider providing resources needed to support each step of the risk management process.**
* **Consider providing information and knowledge management systems to support risk management.**
* **Consider providing risk management procedures and processes.**
* **Consider providing appropriate risk management methods and tools.**
1. Establish internal and external communication plans
* **Establish internal risk management communication and reporting mechanisms.**
* **Establish internal risk management communication and reporting processes.**
* **Develop a plan that describes how you intend to communicate with your organization’s external stakeholders.**
* **Implement your external risk management communication plan.**
1. Implement you approach to Risk Management
* **Develop a strategy to implement your organization’s framework.**
* **Implement your organization’s risk management framework.**
* **Develop a plan that explains how you intend to apply your organization’s risk management process.**
* **Use your risk management plan to implement your organization’s risk management process.**
1. **Monitor your Risk Management framework**
* **Evaluate the ongoing effectiveness of your risk management framework.**
* **Prepare reports on the effectiveness of your risk management framework.**
1. **Improve your Risk Management framework**
* **Study the results of your risk management monitoring and review activities.**
* **Figure out how you’re going to improve yours risk management framework.**

**THE RISK MANAGEMEMT PROCESS**

1. **Apply your risk management process.**
* **Make your risk management process part of your management approach.**
* **Make your risk management process part of your unique culture.**
1. **Communicate and consult with stakeholders during all stages of the risk management process.**
* **Use a consultative team approach to communicate and consult with your organization’s stakeholders.**
1. **Identify and understand the parameters and variables that influence and control how your organization manages risk.**
* **Define your organization’s external context.**
* **Define your organization’s internal context.**
1. **Identify and understand your organization’s external context and consider the influence it could have on its ability to manage risk and achieve its objectives.**
* **Identify and understand environmental conditions and consider the influence they could have on your organization’s ability to achieve its objectives.**
* **Identify and understand key external factors and consider the influence they could have on your organization’s ability to achieve its objectives.**
* **Identify and understand the relationships you have with external stakeholders and consider the influence they could have on your organization’s ability to achieve its objectives.**
* **Consider your external context when you develop your organization’s risk criteria.**
* **Consider the concerns, objectives, and perceptions of external stakeholders when you formulate your risk criteria.**
1. **Identify and understand your organization’s internal context and consider the influence it could have on its ability to manage risk and achieve objectives.**
* **Understand your organization’s internal stakeholders.**
* **Understand your organization’s governance structure.**
* **Understand your organization’s capabilities.**
* **Understand your organization’s culture.**
* **Understand your organization’s standards.**
* **Understand your organization’s contracts.**
1. **Establish the unique context of your risk management process.**
	* + **Adopt a risk management approach that is appropriate to your circumstances and consistent with your context.**
		+ **Identify the organizational areas or parts that will participate in your risk management process and make**
		**sure you understand what they do and how they do it.**
		+ **Clarify how each specific risk management process or activity should be organized and managed.**
		+ **Define the goals and objectives of the risk management activities and projects you intend to carry out.**
		+ **Define the resources that your risk management activities and projects will need.**
		+ **Define the risk management responsibilities and authorities of all process participants.**
		+ **Define the focus of each risk management project including where and when it will be carried out.**
		+ **Define the decisions that will need to be made as you carry out each risk management process.**
		+ **Define the risk assessment methodologies that you intend to use for each risk management process or project.**
		+ **Define how your risk management process is related to your organization’s other processes.**
		+ **Define the studies that you intend to carry out to support each risk management process.**
		+ **Define how risk management process performance and effectiveness will be evaluated.**
		+ **Define the records that each risk management process or activity should maintain.**
2. **Define your organization’s risk criteria.**
	* + **Consider your organization and how it functions when you define your risk criteria.**
		+ **Consider the views of your organization’s stakeholders when you define your risk criteria.**
		+ **Consider the nature and type of causes when you define your risk criteria.**
* **Consider the consequences and impacts that could occur when you define your risk criteria.**
* **Consider how likelihood or probability will be determined when you define your risk criteria.**
* **Consider how the level of risk will be determined when you define your risk criteria.**
* **Consider whether combinations of multiple risks should be taken into account when you define your risk criteria.**
* **Review and periodically update your risk criteria.**
1. **Carry out your risk assessment process.**
* **Identify your organization’s risks.**
* **Analyze your organization’s risks.**
* **Evaluate your organization’s risks.**
1. **Choose suitable risk identification tools and techniques.**
* **Select suitable people to identify your organization’s risks.**
* **Use effective tools and techniques to identify the risks that could affect the achievement of your organization’s objectives.**
* **Generate a comprehensive list of risks that could affect the achievement of your organization’s objectives.**
1. **Analyze the risks that your organization faces.**
* **Estimate your organization’s level of risk.**
* **Specify how much confidence you have in your analysis.**
* **Use your risk analysis to understand your organization’s risks.**
* **Communicate the results of your risk analysis.**
1. **Use the results of your risk analysis to evaluate your organization’s risks.**
* **Use the results of your risk analysis to consider your risk treatment options.**
1. **Establish a cyclical risk treatment process.**
* **Consider your organization’s risk treatment options.**
1. **Select the most appropriate risk treatment options.**
* **Plan the implementation of your risk treatments.**
1. **Document your organization’s risk treatment plans.**
* **Discuss risk treatment plans with all participants.**
* **Carry out your risk treatment implementation plans.**
* **Keep appropriate records of risk treatment activities.**
1. **Plan your risk management monitoring and review processes.**
* **Monitor and review all aspects of your risk management process.**
* **Record your organization’s monitoring and review results.**
* **Report your risk management monitoring and review results.**
1. **Create and maintain records to support your risk management process.**
* **Use your records to support your organization’s risk management process.**

**RISK ASSESSMENT – ISO 31010**

ISO 31010 is a supporting standard for ISO 31000 providing guidance on the selection and application of systematic techniques for risk assessment. Risk assessment carried out using this standard contributes to the effectiveness of risk management practices. A wide range of risk assessment techniques are provided.

The purpose of risk assessment is to provide evidence-based information and analysis to make informed decisions on how to best treat particular risks and how to select between options.

Some of the principal benefits of a performing risk assessment include:

1. Provide objective information for decision makers.
2. Understand the risk and potential impact upon organizational objectives.
3. Quantify and ranking of risks.
4. Contribute to the understanding of risks, in order to assist in selection of treatment options.
5. Identify the important contributors to risks and weak links in your processes, systems and organization.
6. Compare risks in alternative systems, technologies or approaches.
7. Identify and communicate risks and their uncertainties.
8. Assist with determining priorities for health and safety.
9. Rationalize a basis for preventive maintenance and inspection.
10. Post-incident investigation and prevention.
11. Select different forms of risk treatment.
12. Meet regulatory requirements.
13. Provide information that will help evaluate the tolerability of the risk when compared with pre-defined criteria.

### Key Features and Benefits:

1. The 31010 Risk Assessment tools provide guidance on the selection and application of systematic techniques that are fully aligned with the ISO 31000 standard. Using these tools with ISO 31000 will enable an organization to take a coherent approach to risk management.
2. 31010 and 31000 do not replace other risk management standards. They underpin them and enable you to streamline existing risk management processes, helping your organization to save time and money!
3. These standards are written in a generic manner and designed to be used in combination with other standards, thus this standard can be leveraged by any organization no matter their size, type or location.

**CONCLUSIONS**

**When properly implemented and applied, ISO 31000 Risk Management guidelines and the supporting ISO 31010 Risk Assessment tools will help you to:**

1. Increase the likelihood that organizational objectives will be achieved.
2. Improve your organizations ability to identify threats and opportunities.
3. Establish a sound basis for planning and decision making.
4. Help your organization allocate and use risk treatment resources.
5. Improve the overall resilience of your organization.
6. Improve operational efficiency and effectiveness.
7. Encourage personnel to identify and treat risk.
8. Enhance your organizations approach to environmental protection.
Improve the effectiveness of your corporate governance activities.
9. Help minimize your organization’s losses and manage opportunities
10. Improve your risk management controls.
11. Comply with legal and regulatory requirements.
12. Enhance your organization’s health and safety performance.
13. Improve loss prevention and incident management activities.
14. Encourage and support continuous organizational learning.
15. Improve the trust and confidence of your stakeholders.
16. Enhance both mandatory and voluntary reporting.
17. Comply with international norms and standards.

**Epilogue**

The ISO Technical Management Board has approved the transformation of the ISO/PC 292 Project Committee into the new ISO/TC 292 Technical Committee, giving it broader scope. The Technical Committee’s theme is to develop “Risk management — Guidance for the implementation of ISO 31000” and it is expected to be completed by 2014.