WHY ISO 31000 IS IMPORTANT TO ORGANIZATIONS NOWADAYS?
Risk analysis, we make them everyday. Crossing the street, deciding to fasten our seat belt or not, starting early to arrive on time to important appointment. But when it comes to risks that occur in companies, a more formal approach is required. Risk analysis can anticipate problems. By adding risk analysis in key business processes, one can commit to steps that ensure that anticipated problems do not occur or steps that respond if they occur. The time and money can be very crucial. A generic risk assessment process has been defined in ISO 31000. This approach can be applied to all types of risk through any kind of organization.

1) What is ISO 31000?

ISO 31000 using AS/NZS 4360:2004 as its first draft. In 2009, ISO 31000 was issued to widespread acclaim. Today, ISO 31000:2009 remains the international standard on risk management. This document counts 34 pages and provides a generic framework for establishing the context of, identifying, analyzing, evaluating, treating, monitoring and communicating risk. ISO 31000 is the first document published in the ISO 31000 Risk Management series and it also includes:

- The ISO Guide 73:2009, Risk management — Vocabulary, providing the definitions of generic terms relating to risk management and with the help of a uniform risk management terminology aiming to encourage the right approach to the description of activities relating to the management of risk.

2) Why considering this ISO standard while my organization is already adhering to COSO in the context of Sox compliance for example?

ISO 31000 can be considered as an update to COSO that reflects current risk management thinking internationally. However, ISO 31000 does provide a number of relevant advantages compared to COSO:

1. It is more practical
2. It provides more details
3. It explicitly defines the terms
4. It is more clearly written, and easier to understand for CXOs, and risk professionals
5. The information in the standard can be adapted to develop guidelines to assess existing risk management methodologies
6. It provides a foundation for implementing other ISO risk management standards and guidelines

The most significant difference is in the definition of risk for ISO 31000 and COSO ERM (Enterprise Risk Management).

ISO defines risk as the "effect of uncertainty on objectives", highlighting the consequences of uncertainty and therefore popping up a different view of the risk than COSO.

At the other side, COSO ERM defines risk as "the possibility that an event will occur and adversely affect the achievement of objectives." COSO concentrates the effort on the analysis of events rather than the consequences of these events for the organization.

As a consequence, ISO appears better in considering the ‘flow on’ consequences of an event occurring.

3) Making risk part of the Quality Management process

Preventing and correcting unwanted actions and outcomes have long been a part of ISO 9001, but it has been limited to specific elements of the quality management process. ISO 9001:2015 is about to change that.

As an organization, ISO has already addressed the notion of a more global risk management approach to businesses in its ISO 31000 standard, which provides an organizational-level risk management approach. ISO 31000 deals with crucial risk management concepts like:

- When to or not to accept risk when taking advantage of a key opportunity.
- Acceptable ways to remove a risk source entirely
- Avoiding activities associated with a given risk

4) Which additional advantages will I have in adopting the ISO31000 standard?

In addition to ISO 31000, the ISO 31010 introduction provides general principles of risk management. The annexes go into more details on different types of risk assessment techniques explaining the positive and negative aspects of each of them.

For the organization that will have an effective implementation of ISO 31000, the risk management will provide the following advantages:
WHY ISO 31000 IS IMPORTANT TO ORGANIZATIONS NOWADAYS?

- It creates and protects value.
- It is an integral part of all organizational processes.
- It is part of decision making.
- It explicitly addresses uncertainty.
- It is systematic, structured and timely.
- It is based on the best available information.
- It is tailored.
- It takes human and cultural factors into account.
- It is transparent and inclusive.
- It is dynamic, iterative and responsive to change.
- It facilitates continual improvement of the organization.

Conclusions

Managers need to understand the importance of risk management as a tool for meeting business needs and developing management program to support these needs. The objective of Risk Management is to identify, analyze, quantify and manage information (security-related) risks to achieve business objectives through a number of tasks.

Risk management is a process aimed at achieving an optimal balance between realizing opportunities for gain and minimizing vulnerabilities and loss. This is usually accomplished by ensuring that the impact of threats exploiting vulnerabilities is within acceptable limits at an acceptable cost.

Risks affecting organizations can have consequences in terms of economic performance and professional reputation, as well as environmental, safety and societal outcomes. Therefore, managing risk effectively helps organizations to perform well in an environment full of uncertainty.