IMPLEMENTING A RISK MANAGEMENT STANDARD

Constantin PREDA

Risk Manager
NATO Alliance Ground Surveillance Management Agency (NAGSMA),
NATO HQ, Brussels, Belgium

After risk management "conquered" more and more project managers' minds and showed its benefits for business and programs, the need to have a global risk management standard has become a crucial issue in the world of risk management. But having a global risk management standard has been a big challenge, starting from the decision of developing the standard (March-June 2005), to the moment of publishing it, November 2009. So, developing the ISO 31000:2009 standard has been more or less like a bumpy ride. Apparently, the people involved in developing the global risk management standard understood from the very beginning that no challenges are too big, nor any tasks too small and that the task of having a new, comprehensive global risk management standard should be completed with excellence: defining the principles and the framework guiding the risk management process applicable for all type of organizations and for a wide range of activities. Coming up with a global standard should always be based on the real organizations' needs and should fulfill real risk management requirements. The article is trying to present the pros and cons of risk management standard implementation, challenging the implementation process itself and the added value of implementing the standard due to the lack of implementation enablers, like risk culture, a real problem especially in an international environment.

Key words: *standard, implementation, risk culture, ISO, enablers.*

1. THE NEED FOR A RISK MANAGEMENT STANDARD

There was no shortage of the number of standards and guidelines in the area of risk management in the last decade. The large body of standards has grown in an uncoordinated manner, leading to significant inconsistencies and resulting in a lack of a coherent approach and terminology recognized by the Industry. Risk management has been considered first as a system engineering process and after a while a program management process. But the risk management process defined in the ISO/IEC standards (like ISO/IEC 15 288, System Life Cycle Processes, ISO/IEC 12 207 Software Life Cycle Processes, ISO/IEC 24 748 Life Cycle Process Concepts and Definitions) is not enough to be applicable to both engineering and management.

The ISO 9001:2008 contains for the first time requirements indirectly associated with risk management, concerning the management reviews, human resources, infrastructure, and review of requirements related to the product, control of design and development. “Risk management is even more strongly suggested by the ISO 9004, which emphasizes the need for risk management for the development and sustainability of the business in organization. The ISO/IEC Guide 73:2002 provided government and non-governmental organizations with a set of basic definitions and terminology relating to risk management”. [1] However, there was a strong need for an ISO standard that ensures a consistent approach to risk management. “The adoption of consistent processes within a comprehensive framework helps ensure that risk is managed effectively, efficiently and coherently across an organization”. [2]

2. WHAT IS A STANDARD?

There are many definitions of a ‘standard’. Generally speaking, a standard means a set of rules, principles which should be followed in different areas in order to provide coherency, a systematic approach and a kind of predictability in terms of processes, product content, structure and quality.

The International Organization for Standardization (ISO) defines a standard like “a document that provides requirements, specifications, guidelines or characteristics that can be used consistently to ensure that materials, products, processes and services are fit for their purpose”.

More specific, the ISO/IEC Guide 2:2004 (Standardization and related activities - General vocabulary) defines a standard as “a document established by consensus and approved by a recognized body that provides for common and repeated use, rules, guidelines or characteristics for activities or their results, aimed at the achievement of the optimum degree of order in a given context” [3].

The Project Management Institute (PMI) defines a standard as “guidelines for achieving specific project, program and portfolio management results”. In essence, a standard is an agreed way of doing something. It could be about making a product, managing a process, delivering a service or supplying materials. Standards can cover a huge range of activities undertaken by organizations. They can be very specific, such as to a particular type of product, or general such as management practices. Standards generally represent minimum levels of acceptability and are in general voluntary. Even if a standard is not compulsory, many organizations comply with it in order to demonstrate their commitment with the best practices in a specific business area. However, where a standard is touching people health and safety or the environment, it may be compulsory. The government can also make some standards mandatory in relations with specific laws/regulations.

3. RISK MANAGEMENT STANDARD IMPLEMENTATION. PROS AND CONS

It is hard to imagine our world without standards. The products might not work properly, in the way they are expected to work, they will probably have low quality, without being interoperable, compatible with other equipment and sometimes non-standardized products will be even dangerous for the users. Because of the standards the products/services are seen by the Customers as safe, healthy, secure and high quality. ISO standards ensure that products and services are safe, reliable and of good quality. For business, they are strategic tools that reduce costs by minimizing waste and errors and increasing productivity.

Some of the most well-known ISO standards are management system standards. They provide a model to follow by an organization when setting up and operating a management system. Like all ISO standards, they are the result of international experts' consensus and best practices. These standards can be applied to any organization, large or small, whatever its sector of activity.

The risk management standard recommends that organizations should have a framework that integrates the risk management process into the organization's overall governance, strategy and planning, management, reporting processes, policies, values and culture. "Although the practice of risk management has been developed over time and within many sectors to meet diverse needs, the adoption of consistent processes within a comprehensive framework helps ensure that risk is managed effectively, efficiently and coherently across an organization"[2].

For any standard, including a risk management standard, there are pros and cons concerning the benefits of implementing it for the organization, business and customer. Some of the pros and cons concerning the implementation, without entering into details because they are most of the time self-explanatory are highlighted below.

Pros:

- It improves organizations' performances and reduces their risk exposure;
- It supports the implementation of risk management in a formal, process oriented way;
- It ensures that the products and systems are safe, reliable and perform as intended (fit-for-purpose);
- It improves business and management practices;
- It saves business time and money, making business more efficient;
- It provides a great set of tools for examining risks;
- It represents a benchmark for performance evaluation;
- It supports the management decision making process.

Cons:

- It involves additional costs (training, implementation, tools);
- It provides no clear answers to particular organization/business aspects;
- It has no clear corresponding guidelines for supporting the implementation;
- It needs to be revised frequently in response to rapidly changing business circumstances;
- It does not offer the same level of qualifications for international trade as some ISO standards because no certification process exists;
- It does not guarantee the risk management effectiveness;
- There is no pressure in legislation for organizations to comply with the standard;
- The cycle for producing/updating the standard is a long one.

The conclusion is quite obvious in favor of implementing a risk management standard because the standard "provides the principles and guidelines for managing any form of risk in a systematic, transparent and credible manner and within any scope and context" [2]. At the same time the implementation of a risk management standard should not be seen as a way for solving all the problems related to an organization/program risk management process. The standard could be definitively considered as a strong foundation supporting the risk management process but each organization should implement/involved the appropriate risk management enablers which are not all the time within the borders of the standard (**Figure 1**). One of the risk management process enabler is the risk culture and the organization's best management practices producing real results in achieving the business objectives. Standards represent approved or common practice which may or may not be reasonable and so compliance with these standards and codes of practice is a starting point, not a goal.

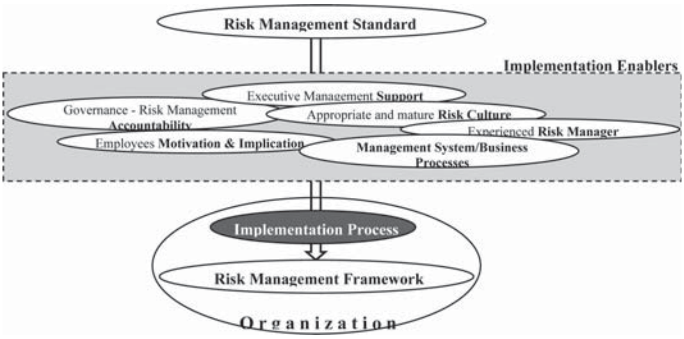
Risk Management Standard
Implementation Enablers
Executive Management Support
Governance - Risk Management Accountability
Appropriate and mature Risk Culture
Experienced Risk Manager
Employees Motivation & Implication
Management System/Business Processes
Implementation Process
Risk Management Framework
Organization

Figure 1. Risk management standard implementation enablers

4. RISK MANAGEMENT BEST PRACTICES

There are quite a lot of private companies which have been accumulated merged and preserved a strong risk culture coming mainly from their leaderships, different stakeholders and business experience. If in this kind of companies the board of directors and top level management can understand, define and actively manage the organization's risk appetite and attitude, the implementation of the best risk management practices is becoming more a technical risk management process implementation issue then a governance issue.

In these companies the risk management process has been developed and refined based on the lessons learned and best practices shared among the practitioners of risk management through the risk management Community of Practice.

Managing risks within this strong and mature environment could be done in a very effective way where the people feel that they have a say and the process is not imposed by someone or based on specific risk management standard requirements. The key for getting the buy-in of the risk management process is to succeed to make the risk management actors understand that the choices came from them and not from an authority imposing rules to be followed. Implementing a risk management standard in these companies should be an easy job with the aim of increasing the risk management maturity level from level 4 (Integrated) to level 5 (Optimized).

5. RISK MANAGEMENT STANDARDS

The first Australian and New Zealand Risk Management Standard, AS/NZS 4360, was released in 1995 and updated in 1999 and 2004 respectively. This standard was increasingly adopted and translated by other countries. AS/NZS 4360:1999. The "Risk Management" standard provided a generic guide for the establishment and implementation of the risk management process involving establishing the context and the identification, analysis, evaluation, treatment, communication and on-going monitoring of risks. The standard specified the elements of the risk management process without enforcing uniformity of the risk management systems. It was generic and independent of any specific industry or economic sector.

Two other risk management standards appeared in quick succession: in 2001 Japan launched a risk management system called JSI Q 2001:2001, which offered two advantages, formal definition of risk management system and the introduction of continuous improvement. In 2002 the UK Institute of Risk Management (IRM) introduced its standard, "A Risk Management Standard".

In 2004 the AS/NZS 4360:2004, "Risk Management" mainstreamed the concept of risk in the 20th century, endorsed a risk management approach covering whole organization, including government, standardized to a certain point the risk nomenclature and it seems to have created a Risk Manager profession and emphasized the importance of 'context'. It also gave the impression that if the standard is followed all will be well and created a focus on assessment rather than driving the attention to risk mitigation. It failed to convince about the multidimensional nature of the risk and the range of concepts and tools required considering it. The Australia and Standards New Zealand supported the development of an international standard which resulted in the publication of ISO 31000:2009 which has been ratified by both countries as AS/NZS ISO 31000:2009 standard with minor changes to the Introduction to address the application of the standard in Australia and New Zeeland.

Canada has also adopted the ISO 31000 Risk Management standard in 2010. "CAN/CSA ISO 31000 Risk Management – Principles and Guidelines" provides a framework and process for managing risk in any public, private, or community organization. Canadian Standards Association (CSA) confirmed that "the Canadian adoption of the ISO 31000 Risk Management standard will enable Canadian organizations to compare their practices with an internationally recognized benchmark, providing them with sound principles for effective risk management". CSA Standards also developed a new edition of its existing risk management standard to supplement the international standard. CSA Q850-10 "Risk Management – Implementation of CAN/CSA ISO

31000" provides further guidance to implementing the international standard taking into account the need of Canadian stakeholders.

A short description of ISO risk management specific standards is provided only for having the whole picture related to their implementation process. It should be noticed that there are two levels of standard scope: project and organization. The risk management standards described below can be adapted for use at organization level and project level.

5.1. ISO 31000:2009, "Risk Management – Principles and guidelines"

The standard serves as a 'peak' standard to harmonize other standards dealing with specific areas of risk management. The standard is built around three fundamental pillars: risk management principles, risk management framework and risk management process. The main variations from the AS/NZS 4360:2004 as outlined in the Introduction of the AS/NZS ISO 31000:2009 are:

- "Risks are defined in terms of effect of uncertainties on objectives";
- The principles to be followed to achieve effective risk management have now been made explicit;
- There is much greater emphasis and guidance on how risk management should be implemented and integrated into organizations through the creation and continuous improvement of a framework;
- An informative Annex describes the attributes of enhanced risk management and recognizes that "while all organizations manage risk in some way and to some extent this may not always be optimal". [2]

The process described for managing risk is identical to that in AS/NZS 4360:2004. The standard is not intended to impose uniformity of risk management across organizations and is not intended for certification, regulatory or contractual use.

5.2 ISO/IEC Guide 73:2009, "Risk management – Vocabulary"

This document, which replaced the earlier 2002 version, provides an extensive set of defined risk management concepts for application in every standard about risk management. Guide 73 is therefore a 'normative' companion document to ISO 31000:2009. As written in the Introduction the "Guide provides basic vocabulary to develop common understanding on risk management concepts and terms among organizations and functions, and across different applications and types" [4].

5.3 ISO/IEC 31010:2009, "Risk management – Risk assessment techniques"

The standard is providing guidance on the selection and application of systematic techniques for risk assessment supporting the implementation of the ISO 31000:2009 standard.

5.4 PMI – Practice Standard for Project Risk Management

Project Management Institute (PMI) risk management standard "describes processes, activities, inputs and outputs for the project specific risk management area. It provides information on what the significant process, tool, or technique is, what it does, why it is significant, when it should be performed or executed and, if necessary for further clarification, who should perform the process” [5].

6. RISK MANAGEMENT STANDARD IMPLEMENTATION

Implementing a risk management standard is a real challenge for many reasons, first of all because it could be something quite new for an organization. The risk management standard needs also to be tailored to the organization’s needs, getting the buy-in from the top management and the support of all the people involved in the risk management process. For some people following a standard seems to be a kind of set of constrains which actually are limiting their freedom in applying the principles and methods they are used with. And in an international environment the situation is even more complicated because of the various risk culture level of knowledge and practices. A risk management standard should support and not suppress the entrepreneurial spirit of an organization.

From quite clear standard provisions to a comprehensive risk management process to be followed with achievable outcomes there is a long way. Fundamentally important for the implementation of a risk management standard is a clear understanding of what the standard means, what it requires and what its implementation involves. The decision for implementing a specific standard is based on the different aspects related to an organization and its business: the business goal/objectives, the business environment, the management system, regulatory requirements, the size of the organization, the program/business complexity, the level of risks and the organization’s risk appetite and tolerance and the list could continue. Some practical considerations should also be taken into account by an organization in order to successfully implement a risk management standard. These include, but are not limited to, the following: organization risk culture, risk maturity level, management commitment and support, people strong motivation and implication and of course the background and experience of the risk manager. The standard implementation should be treated as a project itself.

The implementation of a risk management standard can produce benefits to an organization but it can be a failed process if not all the needed enablers are present. In more practical terms, the key aspect for a successful implementation of a standard is the “buy-in from the others”. Building a carefully “marketing message” for each standard implementation step and trying to make everyone in the organization see the added value for him/her during the daily work is of great importance for the success of standard implementation. If the Stakeholders do not see any added value for their personal work, they will not buy the process and the standard implementation will be in danger. Arguments in favor of standard implementation to be presented to a top manager are very different from the arguments presented to an end user. However, the implementation of a risk management standard could be made even by taking any parts of it and using them at whatever level the organization or project are able to accept. It is better to use at least part of the standard than none at all.

Due to the high cost involved in implementing a standard, many organizations generally hesitate to implement them. Although appointing a consultant may be worthwhile investment for an organization, this is not always necessary. However, many organizations find it difficult to implement the standard without having a consultant. The consultants have the experience, expertise that the organization may not possess and they can offer the latest and objective point of view, bringing the latest and unbiased ideas from their wide experience. The Programme Management Office (PMO) can also be a solution for supporting the risk management standard implementation. Finally, the chosen approach depends on the level of competency available in the organization.

7. RISK MANAGEMENT STANDARD IMPLEMENTATION STEPS

To implement a risk management standard a number of steps should be taken. This will provide clear responsibilities in standard implementation, will allow implementation progress measurement, transparency and will increase people participation and confidence in following the standard.

The steps that should be followed in implementing the risk management standard are described below and the entire process is presented in **Figure 2**:

- Gain executive management level support/buy-in for implementing the standard, including resources;
- Setting up an implementation committee in which the top management should appoint a member of organization's management as management representative. Persons having good knowledge of the organization's processes and good communication-writing skills should be included as members of the committee (the position could be played by the Quality/Knowledge Manager);
- Create an Implementation Plan describing the process, the expertise needed and the roles;
- Provide Training and Technical Support;
- Organize awareness activities for communicating to the people the aim of implementing the risk management standard, the advantages it offers, how it will work, their roles and responsibilities;
- Make sure that the standard based process is in line with the organization processes;
- Develop risk management documents (policy, plan, process, working instructions);
- Get management approval for all the implementation documents;
- Publish and advertise them; get people feedback;
- Implement the risk management process (a trial period can be used);
- Internal audit;
- Management reviews.

Through leadership skills the top management is able to create an environment in the organization where people are fully involved, and in which a risk management system can operate effectively. The top management should demonstrate its commitment and determination to implement the risk management standard. It is important to note that the training and awareness is very important in implementing the risk management standard.

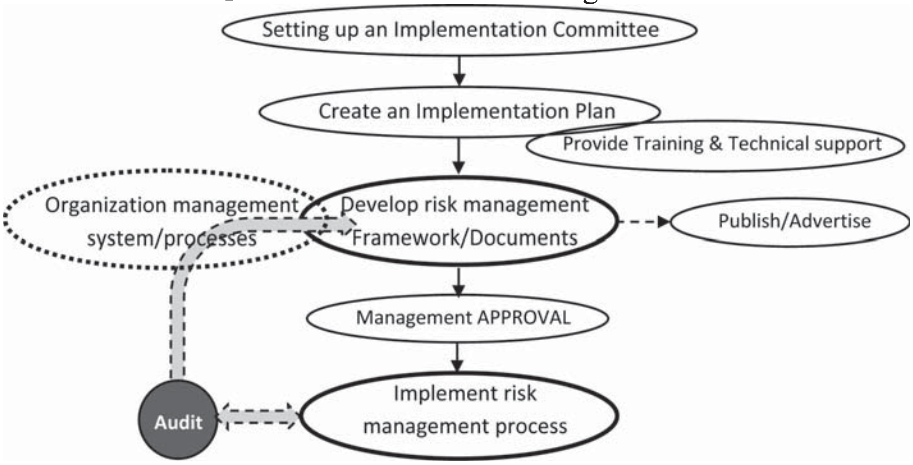
Setting up an Implementation Committee
Create an Implementation Plan
Provide Training & Technical support
Organization management system/processes
Develop risk management Framework/Documents
Publish/Advertise
Management APPROVAL
Audit
Implement risk management process

Figure 2. Risk management standard implementation process

8. RISK MANAGEMENT METHODOLOGIES, HANDBOOKS, GUIDELINES

Risk standard implementation involves sometimes the existence of handbooks, guideline or methodologies as a support in better understanding the standard provisions but also as a roadmap describing the steps and the direction to be followed for a comprehensive and effective risk management standard implementation.

A methodology is considered to be a collection of proved steps to be followed for achieving a result in different business/project areas. A methodology is normally a well designated and documented procedure providing practical processes for getting the risk management standard implementation done.

For some organizations it is considered to be much easier and best value to follow a specific risk management methodology, like PRINCE 2, than to spend resources for implementing a standard. The methodology provides specific steps and project key points where the risk management is necessary.

The roles and tasks of different entities involved in the risk management process are well defined. The specific risk management documents (Risk Log, reports) and their corresponding project management documents are specified and provided as templates. A risk management methodology can be adopted from a standard, like ISO 31000:2009, but a standard will never ever be a methodology.

Handbooks are generally intended to provide more information that assists in the application of a particular standard. The guideline related with risk management standards can provide explanation and guidance on the application of the standard, including detailed advice on each step of the risk management process. One of this, "A Structured Approach to Enterprise Risk Management (ERM) and the Requirements of ISO 31000", has been published by IRM, AIRMIC and Alarm, which provides up to date guidance on the implementation of Enterprise Risk Management in the context of the new ISO 31000:2009 standard.

9. INTERNAL AUDIT

As per the requirement of ISO 9001:2008 QMS Standard, the organization needs to conduct internal audits at planned intervals. The audit purpose is to ensure that the risk management system conforms to the planned objectives and to the requirements of the risk management standard and to those established by the organization. Even after the system stabilizes and starts functioning, internal audits should be planned and performed as a regular strategy. The non-conformances pointed out in the internal audit should be resolved by ensuring corrective actions and conformance.

10. CONCLUSIONS

The implementation of the risk management standard is a complex task. The added value gained through the implementation of the risk management standard is directly impacted by the executive management and the contributors to the risk management system in terms of risk culture, process and experience. The risk standard is not implemented by robots but people and human psychology plays a major influence. Finally the risk attitude is the key because it drives the risk behavior and risk culture.

ISO 31000:2009 it is not a complete answer to dealing with risk in organizations but it is a big step forward. However, the development of ISO 31004, Risk Management-Guidance for the implementation of ISO 31000 should not be postponed, even years from this point in time. The purpose of ISO 31004 to address the ISO 31000 Achilles Heel and make it work in a practical way should get the risk experts' support across the globe. The risk management standard will gain power when it will be a pressure in legislation for organizations to establish effective risk management and corporate social responsibility control.

REFERENCES

[1] Evgeny Avanesov-Risk Management in ISO 9000 series standards, International Conference on Risk Assessment and Management, 24-25 November 2009, Geneva.

[2] AS/NZS ISO 31000:2009, Risk management principles and guidelines.

[3] ISO/IEC Guide 2:2004, Standardization and related activities - General vocabulary.

[4] ISO/IEC Guide 73:2009 Risk management – Vocabulary.

[5] Project Management Institute (PMI) - Practice Standard for Project Risk Management.