

ANALYSIS OF INTERNATIONAL RISK MANAGEMENT STANDARDS (ADVANTAGES AND DISADVANTAGES)

Remzi Ahmeti
Raifeissen Bank
KOSOVO

Besarta Vladi
European University of Tirana
ALBANIA

ABSTRACT

Recent year's study of the risk management has become an important discipline in the field of management. Risk Management is a central element in any organization's strategic management. Basically, risk management is the process where an organization tries to address the most potential risks associated with its activities. A successful risk management should address and identified risk, be associated with other organizational activities, should be part of routine and dynamic activities, responding in a timely and on appropriate manner ,to any changes that the organization may experience (AIRMIC, ALARM, & IRM, 2010). This work seeks to analyze International Risk Management Standards and the role of implementing these standards on performance improving of the organization. The document is based on the interpretation of secondary data such as studies, reports and ISO standards for risk management.

Keywords: Risk, risk management, international risk management standard.

INTRODUCTION

Risk and its management is not a voluntary choice for the organization, risk is simply a threat or an opportunity to be managed in order to ensure the achievement of business objectives. Each business activity faces a risk and the management of these risks at the organization level helps to achieve the objectives of the enterprise. Risk should always be managed in order to ensure that potential negative consequences are avoided or eliminated as much as possible, or that the business benefits from all the opportunities it offers to the environment in which it operates. In recent years, many public companies around the world have invested heavily in enterprise risk management increase (the Swedish National Audit Office, 2015). One of the most important contributors to risk management is related to the implementation of the ISO standard 31000.

LITERATURE REVIEW: INTERNATIONAL RISK MANAGEMENT STANDARDS

Numerous efforts have been made to standardize terminology and risk management procedures. The focus of this study will be the treatment of the most recent international standard, ISO: 31000. Published in 2009, this standard has found an application widely in sectors and in different countries (ISO, 2017). ISO is an internationally renowned organization for its standards that have historically found high acceptance, such as the ISO 9000 Quality Management Standard, and ISO 14000 on Environmental Management (Su, Zhao & Tan, 2015). The high reputation of the organization as well as the broad global acceptance of previous standards made the publication of the standard on Risk management to be welcomed and very fast began to replace the many standards used in Risk Management.

Table 1: Key standards of the risk management

Standards	Short description
ISO 31000	Published by the International Standards Organization (ISO) (2009)
BS 31100	British standard, published by the British Standards Institute (2008)
Institute of the risk Management (IRM)	Standard published by AIRMIC, Alarm and IRM(2002)
COSO ERM	Framework published by the Committee of Sponsoring Organizations of the Tread way Committee (2004)
Turnbull Report	Framework published by the Financial Reporting Council (2005)
Orange Book	Standard published by the HM Treasury of the UK government(2004)
CoCo (control criteria)	Framework published by the Canadian Institute of Chartered Accountants (1995)
Source :	
(AIRMIC, ALARM, & IRM, 2010)	

Risk Management Standard was prepared by the ISO Technical Management Based Working Group and its design has been selected by experts from 28 different countries and specialists from several organizations (Purdy, 2010). The reach of a consensus has lasted about 4 years and more than seven drafts of the standard have been prepared. Drafts were cast for voting by board members and a minimum approval of 75% was required in order for the standard to be published (ISO, 2017). The standard does not mention other work and consequently the origin of many concepts remains unknown.

METHODOLOGY

This study has an exploratory nature and aims to gather enough information about the role and contribution of international ISO standards in managing the risk of the organization, taking into account the advantages and disadvantages of this standard. The work is an analytical, mainly based on secondary data analysis as well as on the interpretation of ISO standards in the function of risk management in the organization.

The purpose of this work is to undertake a depth analysis of risk management based on ISO international standards.

The ISO standard classifies the risk into three categories:

- Risk as a threat (a pure risk)
- Control Risk (or Insecurity)
- Risk Opportunity (or speculative),

The basic research question of this study is: How did international ISO standards influenced a better risk management in the organization?

The basic hypothesis of the study is: Implementation of ISO standards in terms of risk management has positively impacted on minimizing the negative effects of the risk on the organization

RESULTS & DISCUSSIONS: ADVANTAGES OF THE ISO 31000 STANDARD

Many of the principles of the standard ISO 31000 are similar to the previously published risk management standard AS / NZS 4360: 2004, published by Standards Australia in conjunction with the New Zealand Standards. However, ISO standardization gives a new definition of risk and 11 risk principles that are not presented in AS / NZS4360

The eleven risk principles proposed by ISO are:

1. Risk management creates value.

2. Risk Management is an integral part of the organization's processes.
3. Risk management is part of decision-making.
4. Risk management clearly addresses insecurity.
5. Risk management is systematic, structured and programmed.
6. Risk management is based on the best available information (accessible).
7. Risk management is tailored.
8. Risk management takes into account human and cultural factors.
9. Risk management is transparent and inclusive.
10. Risk management is dynamic, iterative and responsive to change.
11. Risk management facilitates continuous improvement.

The purpose of the ISO 31000 standard is to provide general guidelines for creating a risk management framework, in the context of which risk management is applied. This standard is applicable to any organization, regardless of sector or size.

At present, the standard is organized into three main separate volume related to risk management, which is:

- ISO 31000: 2009 - Principles and Guidelines on Implementation
- Guide ISO 73: 2009 Risk Management- Dictionary
- ISOMEC 31010: 2009 - Risk Management - Risk Assessment Techniques

Principles and guidelines ISO 31000 provides the main contribution from this standard, while the other two volumes are more like additional information on these principles and guidelines. The publication of principles and guidelines includes a description of risk management principles, risk management context, and risk management process. Concepts of principles, context and risk management process are also known as risk management architectures. Also, the context of risk management refers only to a specific part of the Principles and Guidelines of this Standard (ISO 31000: 2009). Overall in the literature on risk management the concept of risk management context refers to the standard of risk management.

Different from the ISO standard, other first standards are focused on the risk management process, ignoring other supporting documents that help to manage the risk management process.

The part of the standard relating to risk assessment titled ISO 31010: 2009, Risk Management - Risk Assessment Techniques, Includes techniques that can be applied in Risk assessment. These techniques are based on the implementation of the principles and guidelines proposed by this standard. The risk assessment techniques are intended to assist in the implementation of the ISO 31000 standard. It includes some well-known and applied assessment techniques in the literature, such as scenario analysis and HAZOP. Consequently, the aspect of the standard contribution to risk assessment and related techniques is not that it provides a great scientific and practical contribution. However, the techniques presented by this standard are not addressed in detail and specific in this research, for the fact that they are simply a reflection of the main material of this Standard, Principles and Guidelines.

Regarding the "ISO Guide 73: 2009 - Risk Management - Dictionary" This is an explanatory dictionary of the terminology used in the risk management standard, including definitions for a number of concepts used in risk management. ISO 73: 2009 has aimed at replacing the previous risk management dictionary published by the ISO in 2002, also known as the ISO / IEC Guide 73: 2002.

The ISO 31000 standard is considered as a synthesis of best practices on risk management, referring to several previous Standards such as AS/NZS 4360: 2004 and COSO ERM. The Australian and New Zealand standard, AS / NZS, has been a major contributor to design the ISO standard 31000. Although the ISO 31000 standard has gained popularity in both Australia and New Zealand, this standard has not managed to completely replace AS/NZS standard. The ISO standard has particularly found a very high applicability in Finland.

Another project by ISO was initiated in 2011 in order to prepare a new document that will be added to the 2009 standard, which will be a guide to the new implementation of this standard. The name for this publication, or if it may be called different for this new standard is ISO 31004: Risk Management - Guidance for the Implementation of ISO 31000.

In 2013, this guide was published and ISO/TR 31004: 2013. This publication provides a structured approach to how organizations can shift from their practices to the implementation of the ISO standard, an explanation of the concepts of ISO 31000, and guidance on the respected aspects of risk management principles and guidelines.

ISO / TR 31004: 2013 can be used by any public / private organization or group of individuals.

ISO / TR 31004: 2013 is not specific to any industry or sector, or any type of organization or type of risk; Consequently it can be applied to all types of activities and organizations. The main objective of ISO 31000 is to provide a general guide to risk management. The group that has been involved in the design and publication of this standard has stated that this standard is applicable to any kind of risk, regardless of the nature or expected impact of the organization. Also, according to them, this standard can be applied both in the private and public sectors. According to this standard, the applicability of these principles and guidelines does not have a certain duration, but is developed throughout the organization's lifetime.

Given that this ambitious approach to managing any risk in any kind of situation and everywhere, this standard does not provide a detailed guide on how a local public authority in the public sector should manage the risk. Indeed, this standard aims to provide the ideal risk management system (Leitch, 2010). With a purpose to provide standard, easier application and more understandable. ISO 31000 is designed based on principles of risk management. This come as result of the facts to categorized risk architecture according to ISO 31000 and does not broad and general, so the standard can be found to be applicable in every context. Unlike many other ISO standards, the ISO 31000 risk management standard does not refer to certification. This is due to the fact that the risk management architecture is fully integrated into the existing management structures and consequently its implementation is unique depending on the organization's typology. Under these conditions, certification of these unique approaches would simply be impossible.

The publication of principles and guidelines is organized in five main parts. The first part introduces the purpose and objectives of the standard. The second part defines the risk management terminology (based on Guide ISO 73: 2009). Part Three, introduces effective principles for risk management. The fourth part describes a model for adjusting the risk framework and the last part presents the risk management process.

RESULTS & DISCUSSIONS: DISADVANTAGES OF ISO 31000 STANDARD

Different authors have critically examined ISO standard 31000, (Aven, 2012) criticizing the terminology used for uncertainty and risk. According to Aven, the guide fails to provide clear and meaningful definitions of these concepts. (Leitch, SO 31000: 2009, the new International Standard on Risk Management, 2010) goes further with the criticisms, stating that the standard is unclear and there is a lack of empirical bases. He justifies the ambiguity of the standard as related to the way it is drafted, by a group of experts gathered from around the world and speaking different languages. (Lalonde & Boiral, 2012) also identify some standard deficiencies by applying this standard to crises that have occurred in the past. The conclusion they come to is that adapting the risk management guide is not as important as it is the decision taken by the managers to address the risks identified.

CONCLUSIONS

In conclusion, ISO 31000, besides being a very effective tool for enterprise risk management, is also applicable as a base for more specialized standards. Consequently, it is important that these standards have the same basis or comparable to the ISO 31000 standard, especially in terms of the vocabulary and terminology used.

The creation of ISO 31000 is motivated in particular by the fact that the risk management industry has always applied a variety of standards for risk management and also the terminology used has been unmet standard thus making communication of risk information more difficult. Despite the numerous of criticism's of this standard, its contribution to better risk management in the organization remains indisputable

REFERENCES

- AIRMIC, ALARM, & IRM. (2010). *A structured approach to Enterprise Risk Management (ERM) and the requirements of ISO 31000*. London. Gjetur në <http://www.ferma.eu/app/uploads/2011/10/a-structured-approach-to-erm.pdf>
- ISO. (2017, 04 23). *ISO 31000 - Risk management*. Gjetur në International Organization for Standardization: <https://www.iso.org/iso-31000-risk-management.html>
- Lalonde, C., & Boiral, O. (2012). Managing risks through ISO 31000: A critical analysis. *Risk Management, 14*(4), 272-300.
- Leitch, M. (2010). ISO 31000:2009—The New International Standard on Risk Management. *30*(6), 887–892. doi:10.1111/j.1539-6924.2010.01397.x
- Leitch, M. (2010). SO 31000:2009—The New International Standard on Risk Management. *Risk Analysis, 30*(6), 887-892. doi:10.1111/j.1539-6924.2010.01397.x
- Purdy, G. (2010). ISO 31000:2009—Setting a New Standard for Risk Management. *Risk Analysis Journal, 30*(6), 881-886. doi:10.1111/j.1539-6924.2010.01442.x
- Su, Y., Zhao, F., & Tan, L. (2015). Whether a large disaster could change public concern and risk perception: a case study of the 7/21 extraordinary rainstorm disaster in Beijing in 2012. *78*(1), 555–567. doi:10.1007/s11069-015-1730-x
- Swedish National Audit Office. (2015). *The Government's management of risk in state-owned enterprises*.