International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878 (Online), Volume-8 Issue-2, July 2019

Modelling Risk Management Process According to ISO Standard

Ikram Akkiyat, Nissrine Souissi

Abstract*: Risk management is defined as an essential step in the improvement process proposed under the standard ISO 9001: 2015. The guidelines to the process of risk management have been proposed since 2009 by the International Standardization Organization (ISO). But before, organization and institutions have their own way to manage risk. An analysis of risk management processes in the literature has been realized in order to identify the standard process. Unified Modeling language (UML) was used to present this meta model. The purpose of this paper is to propose a risk management process model based on ISO 31000: 2018 and following the recommendations of ISO 9001: 2015 by integrating risk management modeling in process modeling.

***Index Terms*: Process Modelling; Model; UML; Risk Management Process; ISO Standards; ISO 31000:2018; ISO 9001:2015;**

I. INTRODUCTION

The term "risk in an organization represents the effect of uncertainty on objectives [1], and its management is an essential step in order to optimize and improve the processes composing the whole system. Risk management is part of the process of the strategic management in an organization, taking into account the importance of the contributions and the influence of the environment. Risk management is defined as the set of coordinated activities to direct and control an organization with regard to risk [1]. Before that ISO (International Standardization Organization) offered a standard of management of risk in 2009, agencies had used different methods to manage risks within their entities. In 2015, the risk management has been recommended by the ISO9001: 2015 as being an important step in the improvement process of an organization. It relies on the definition, assessment and implementation of corrective actions in order to avoid or correct the consequences of the risk. In this paper, we propose a meta-model of risk management process, based on the standard ISO 31000: 2018, which will facilitate the implementation of the risk management process in any type of business process and in any field and in any domain of organizations. We suggest in this sense to follow the recommendations of ISO 9001: 2015 and integrate risk modelling in business process modelling.

This work is organized into five sections; in the second section we present an overview of the different approaches that describe the activities of several risk management processes. A comparative analysis of these approaches is presented in the third section. The fourth section concerns the building of our risk management process meta-model. We finish this paper by a conclusion and perspectives.

II. OVERVIEW OF RISK MANAGEMENT APPROACHES

In this section, we present the main approaches addressing the risk management, such as: the standards ISO 9001: 2015, ISO 21500: 2012, ISO 27001: 2013, ISO 20000-1: 2011 and ISO 31000: 2018 risk management standard. In addition to these standards, we are presenting demarches proposed by PMBOK 6th Edition, NIST (National Institute of Standards and technology - USA) and HSE (Health and Safety Executive - UK). The ISO 31000 standard provides principles and guidelines on risk management. This standard has become a generic and recognized reference for risk management. The standard ISO 31000: 2018 can be used for any field, it is not specific to an industry or a sector [2] [3].The international community involved in its review recognizes its importance and its positioning with regard to its guidelines and its unifying purpose. It seems to be complementary to the different standards applicable to any sector, such as ISO 9001, and can easily allow the implementation of a risk management system.

Other ISO standards, which at the base are not dedicated to risk management, had integrated in their latest editions, a risk-based approach.

The concept of risk in the ISO 9001 standard has been implicit in previous editions, and it is explicit in the 2015 edition [4]. We emphasize here that ISO 9001: 2015 provides requirements for quality management systems, and is aligned with the changes that organizations face, focusing more on performance, reflection based on risk and activation of the cycle Plan-Do-Check-Act at all levels of the organization [4].

In the same way as the ISO 9001:2015, ISO 21500:2012 provides a process for risk management in the framework of the project lifecycle [5]. This international standard provides a high-level description of the concepts and processes considered as good practices in project management.

Revised Manuscript Received on 30 July 2019.
***** Correspondence Author
Ikram Akkiyat*, SIWEB Team, Ecole Mohammadia Des Ingénieurs, Mohammad V University of Rabat, Rabat, Morocco;
Nissrine Souissi, Computer Science Department Rabat School of Mines, Rabat, Morocco & SIWEB Team, Mohammadia School of Engineering, Mohammed V University, Rabat, Morocco

This standard is included as Part II of the PMBOK. It is admitted that the PMBOK Guide [6] had a great influence on the development of the ISO 21500. In this context, as in PMBOK, risk management is present during the process of planning, implementation, and control of the project lifecycle.

The process of assessment and treatment of risks related to information security in ISO/IEC 27001 aligns also with the principles and guidelines in the ISO 31000. ISO / IEC 27001 is the most well-known of the standards of the family ISO 27000, which aims to assist organizations in the field of information security. ISO/IEC 27001 provides the requirements for an information security management system, and includes people, processes and information systems by applying a risk management process [7].

ISO/IEC 20000-1 which is a service management system standard, cites ISO 31000 as the generic reference to risk management [2]. The requirements that provide ISO 20000-1:2011[8]include design, transition, delivery and improvement of services to meet the agreed requirements.

The National Institute of Standards and Technology (NIST) [9]proposes a method of risk management through the proposal of several activities similar to those proposed in the framework of ISO 31000:2018 [9]. It's about framing risk, assessing, proposing solutions and finally risk monitoring.

The Health and Safety Executive [11] proposes a risk assessment process consisting of five activities: Identification of probabilities, assessment of risks and proposal of solutions and precautions, saving important data and finally reviewing the assessment and repeating the process if necessary.

III. COMPARATIVE ANALYSIS

In this section, we present a comparative analysis of the approaches presented in the previous section, and we discuss the results of this analysis.

A. Analysis

A comparative analysis of standards covering the management of risks has been presented in [2], where it was question to compare the activities of the risk management process in the standards ISO 9001, ISO 21500, ISO/IEC 27001 and ISO/IEC 20000-1, and show that an approach of risk management based on the process approach may constitute a basis for the improvement, coordination and interoperability of the activities of risk management in IT, in order to achieve several aspects, such as: project management, quality management and the security of information systems. We present in what follows an enriched version which compares all approaches cited in the previous section, with the process of management of the risks defined in ISO 31000:2018.

The standard ISO 31000:2018 contains 10 chapter, we are here focusing on the 6th chapter which is "Process", since this new release in organized as a High Level Standard (HLS). Table 1 shows the comparative analysis:

Table I: Comparison of different risk management processes

	Risk Management processes							
	ISO 31000:2009	***ISO 9001:2015***	***ISO 21500:2013***	***ISO 20000-1:2011***	***ISO/IEC 27001:2013***	***PMBOK 6th Edition***	***NIST***	***HSE - UK***
Processes' activities	**6.2 Communication and consultation**	4.2 Understanding the needs and expectations of interested parties	4.3.40 Manage communications		4.2 Understanding the needs and expectations of interested parties			
	5.3 Scope, Context and criteria				4.1 Understanding the organization and its context	1. Plan Risk Management	1. Frame the risk	
	6.3.2 Defining the scope		3.11 Project constraints					
	6.3.3 External and Internal Context	4.1 Understanding the organization and its context						
		A.8 Control of externally provided processes, products and services	3.5.2 Factors outside the organizational boundary					
	6.3.4 Defining risk criteria							

	5.4 Risk assessment			6.3.1 Service continuity and availability requirements 6.6.1 Information security policy	6.1.2 Information security risk assessment 6.2 Information security objectives and plans to achieve them 8.2 Information security risk assessment (operation)		2. Assess the risk	
	6.4.2 Risk identification	6.1 Actions to address risks and opportunities (6.1.1)	4.3.28 Identify risks	6.6.3 Information security changes and incidents	6.1.2 Information security risk assessment (c)	2. Identify Risks		1. Identify the hazards
	6.4.3 Risk analysis	9.1.3 Analysis and evaluation	4.3.29 Assess risks		6.1.2 Information security risk assessment (d)	3. Perform Qualitative Risk Analysis 4. Perform Quantitative Risk Analysis		2. Decide who might be harmed and how
	6.4.4 Risk evaluation	9.1.3 Analysis and evaluation	4.3.29 Assess risks		6.1.2 Information security risk assessment (e)			3. Evaluate the risks and decide on precautions
	6.5. Risk treatment	6.1 Actions to address risks and opportunities (6.1.2)	4.3.30 Treat risks		6.1.3 Information security risk treatment 8.3 Information security risk treatment		3. Risk response	
	6.5.2 Selection of risk treatment options				6.2 Information security objectives and plans to achieve them	5. Plan Risk Responses		3. Evaluate the risks and decide on precautions
	6.5.3 Preparing and implementing risk treatment plans					6. Implement Risk Responses		
	6.6 Monitoring and review	9.1.3 Analysis and evaluation 9.3.2 Management review inputs 10.2 Nonconformity and corrective actions	4.3.31 Control risks		9.3 Management review (e)	7. Monitor risks	4. Monitor risk	5. Review your assessment and update if necessary

	6.7 Recording and reporting							4. Record your significant findings

A. Discussion

The comparative analysis confirms the choice of the standard ISO 31000:2018 as a standard of risk management. In fact, by analysing the different activities of the risk management process proposed in the framework of the standards ISO 9001:2015, ISO 21500:2012, ISO 27001:2013 and ISO 2000-1:2011, we can say that the standard ISO 31000:2018 presents the overall process of risk management in all areas. Note that the selected approaches do not describe the activities "communication and consultation" and "Identifying risk criteria".

The process proposed in the framework of the PMBOK corresponds in its entirety to the one of ISO 31000:2018, except that the latter gives more details, especially in the first activity (setting the context), and insists on the revision of the risk after its control.

The process proposed by NIST is similar to the process of ISO 31000:2018. It also proposes a contextualization of the risks. We note that the risk management process in ISO 31000:2018 requires in the stage of evaluation, an evaluation of the results of the analysis of the risks before moving to the treatment, while the process proposed by NIST uses the result of the analysis directly to seek solutions. Concerning the risk treatment, ISO 31000:2018 adds a specific activity that aim to accept or not the solutions/plans for the proposed treatment. Finally, ISO 31000:2018 requires also a control not only of risks, but also of the process in its entirety, and also insists on risk review [10].

The Committee HSE proposes only a process of risk assessment, which is, in its entirety, in agreement with the phases risk assessment and risk treatment proposed in the framework of ISO 31000:2018.

We retain in this work the risk management process proposed in the framework of ISO 31000:2018 and we build in the following section the meta-model that captures all the knowledge relating to this process.

IV. RESULTS

As result of the previous analysis and the presented discussion, we propose a risk management meta model where all the activities proposed in ISO 31000.2018 will be presented.

To build our meta-model, we've based our study on the guidelines of ISO 31000:2018. The ISO standard 31000:2018 proposes in Chapter 5, five main activities dedicated to the risk management process [3], and each activity is composed of several sub-activities. We have defined the rules of management to determine the relationships between these activities.

- The risk management process is described by a set of activities, which are:

(1)Communication and Consultation

(2)Risk assessment preparation: (i) establish the domain; (ii) establish the context; (iii) define risk criteria.

(3)Assess risks: (i) identify the risks; (ii) analyse the risks; (iii) evaluate the risks.

(4)Treat the risks: (i) select the options for risk treatment; (ii) prepare and implement plans.

(5)Reporting:

(6)Risk monitoring and review.

- The first activity which concerns the communication and consultation represents a basis for other activities of the risk management process.
- The third activity (risk assessment) uses the criteria defined in the second activity (Risk criteria) to identify risks.
- After analysis and assessment of identified risks, the result is used to propose and implement responses/solutions.
- In the last activity, monitoring and review, an improvement of the risk management process is imposed.

Fig.1 presents the proposed meta-model of risk management process.

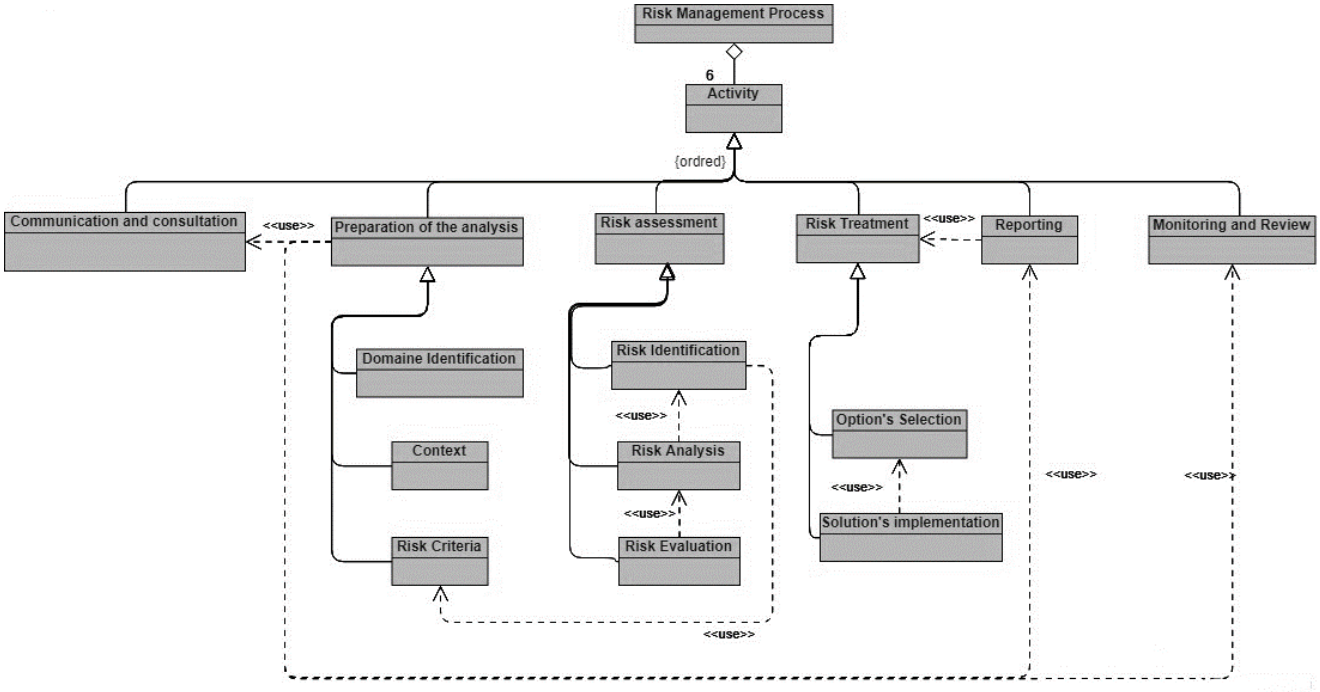


Fig. 1: Risk Management Process Meta model

As shown in the meta model, each activity uses the artefacts of the previous activity, this use is modelled by the "use" relationship. Below a table that explains each use:

Table 2: explanation of the "use" relationships

Use	Description
Preparation of the analysis => Communication & consultation	The activity Preparation of the analysis exploits the data of communication & consultation to identify the domain, the risk criteria and the context
Preparation of the analysis => Monitoring and review Preparation of the analysis => reporting	in a concept of continuous improvement, the artefacts of "monitoring and review" and "reporting" are used a basis of the analysis at every iteration
Risk identification => Risk criteria	The identification of risks is allowed and based on the criteria that are collected and fixed in the "Risk criteria" phase
Risk Analysis => Risk identification	The risk analysis uses the list of risks identified in "Risk identification" as basis
Risk evaluation => Risk analysis	The evaluation of risks is based on the results of risks analysis
Solution's implementation => Options' selection	The implementation of the proposed solutions is based on the options that have been selected in the "Options' selection" activity.

The purpose of this proposal is to provide a process meta-model that takes into consideration the risk analysis and management, based on an international standard, via the creation of a system of risk management integrated in the continuous improvement process. This meta-model will introduce the creation of a risk & opportunity repositories that can help in the establishing of a self-learning system and that can be upgraded to a global risk management system that is enriched with new risks & opportunities and the solutions proposed. This proposal could the meta model extended for improvement cycle in a SoS context [12] that describes the artefact "Risk" in the PLAN phase, which is a recommendation of ISO9001:2015. Another version of improvement cycle meta model was introduced in [13] [14].

V. CONCLUSION

Risk management is a very important phase; it allows the minimization of risk effects sometimes very serious, and ensures an improvement and optimization of the process. The process of risk management must absolutely be integrated in the life cycle of each process, which will facilitate the research of solutions in case of problems.

We have proposed a meta model of risk management process, based on ISO 31000:2018, after realizing a literature review of the risk management processes already proposed. The objective of this standard is to provide the principle guidelines of risk management as well as the process of implementation at a strategic and operational level. UML was used to model this process because in this paper we are aiming to introduce a risk management system, and this meta-model will serve as a guide for the implementation of risk management process.

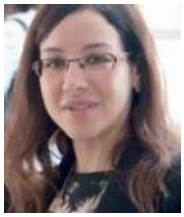
The proposed meta-model will allow process responsible to keep a continuous survey and monitoring on risks and proposed solutions collected during process iterations, by storing them in a repositories and then create a risk management system updated at each improvement, which is required by the risk management standard.

REFERENCES

1. ISO, “ISO Guide 73 :2009 Risk management–Vocabulary,” 2009. [Online]. Available: https://www.iso.org/standard/44651.html.
2. Barafort, A. L. Mesquida and A. Mas, "Integrating Risk Management in IT settings from ISO Standards and Management Systems Perspectives," *Computer Standards & Interfaces*, 2016.
3. ISO, “ISO 31000 :2018,” 2018. [Online]. Available: https://www.iso.org/obp/ui/fr/#iso:std:iso:31000:ed-2:v1:fr. [Accessed MAY 2019].
4. S. Markovic, J. Ruso and A. Horvat, "FMEA Application In Risk Management As Response To The Iso 9001:2015 Requirements," in *Symorg 2016*, Zlatibor, Serbia, 2016.
5. ISO, "ISO 9001:2015: Systèmes de management de la qualité -- Exigences," 2015. [Online]. Available: https://www.iso.org/fr/standard/62085.html.
6. ISO, "ISO 21500:2012: Lignes directrices sur le management de projet," 2012. [Online]. Available: https://www.iso.org/fr/standard/50003.html.
7. Guide to the project management body of knowledge, Project Management Institute, 2017.
8. ISO, "ISO/CEI 27001:2013: Technologies de l'information — Techniques de sécurité — Systèmes de management de la sécurité de l'information — Exigences," 2013. [Online]. Available: https://www.iso.org/obp/ui/fr/#iso:std:iso-iec:27001:ed-2:v1:fr.
9. ISO, "ISO/IEC 20000-1:2011 Technologies de l'information -- Gestion des services -- Partie 1: Exigences du système de management des services," 2011. [Online]. Available: https://www.iso.org/fr/standard/51986.html.
10. NIST, "The National Institute of Standards and Technology," [Online]. Available: https://www.nist.gov/.
11. M. Metheny, Federal cloud computing Second Edition : The Definitive Guide for Cloud Service Providers, Elsevier, 2017.
12. HSE. [Online]. Available: http://www.hse.gov.uk/. [Accessed 2017].
13. Akkiyat and N. Souissi, "Building a Process Meta Model Extended for Cycles," in *ArabWIC 2019*, Rabat, 2019.
14. AKKIYAT and N. SOUISSI, "Process Meta Model extended for the improvement in a SoS Context," in *4th Edition of World conference on Complex Systems*, Ouarzazate, 2019.
15. AKKIYAT and N. SOUISSI, "Improvement View: Extension of Seven Views Approach," in *ISCV*, Fez, 2017.

AUTHORS PROFILE

Ikram AKKIYAT is an engineer, graduated from the High National School of Mining in Rabat (ENSMR). Currently, Mrs. AKKIYAT is a PhD student and member of the SIWEB Team at Mohammadia School of Engineers (EMI), Mohammed V University in Rabat, researching about Business Process Improvement.



Nissrine SOUISSI is a fulltime professor at the MINES-RABAT School, Morocco. She obtained a Ph.D. in computer science from the UPEC University in 2006, France and an Engineer degree from Mohammadia School of Engineers in 2001, Morocco. Her research interests include process engineering, business process management, databases, data lifecycle, smart data, hospital information system, and information system.