Computer and Information Science; Vol. 12, No. 3; 2019
ISSN 1913-8989 E-ISSN 1913-8997
Published by Canadian Center of Science and Education

Information Systems Risk Management: Litterature Review

Soumaya Amraoui[1], Mina Elmaallam[1,2,3], Hicham Bensaid[3] & Abdelaziz Kriouile[1]

[1] IMS Team, ADMIR Laboratory, ENSIAS, Mohammed V University, Rabat, Morocco

[2] LYRICA Laboratory, School of Information Sciences, Rabat, Morocco

[3] STRS Laboratory, Institut National des Postes et Télécommunications, Rabat, Morocco

Correspondence: Mina Elmaallam, University in Rabat, Faculty of Sciences, ENSIAS, BP BP 713, Rabat, Morocco. E-mail: elmaallam@gmail.com

Received: Apirl 1, 2019 Accepted: May 10, 2019 Online Published: June 17, 2019

doi:10.5539/cis.v12n3p1 URL: https://doi.org/10.5539/cis.v12n3p1

Abstract

The security of a company's information system (IS) is an important requirement for the pursuit of its business. Risk management contributes to the protection of the IS assets. It saves the organism from the losses caused by the emergence of unwanted events having an incidence on the IS objectives and consequently on its strategy. It has also an important role in the decision making about entering new opportunities. In addition, it promises an optimal allocation of information system resources. The risk management process aims to analyze what can happen and what are the eventual consequences for the organization before deciding what needs to be done and reducing the risks to an acceptable level. This paper presents a literature review of IS risk management and gives a comparative analyse of its processes, methods and standards.

Keywords: information system, risk management, risk, information system security risk

1. Introduction

Risk management is an extremely important discipline in the governance of information systems. It can help organizations with optimizing their costs insofar as dealing with incidents requiring often more effort than avoiding them (McKeen & Smith, 2003). However, it presents a set of challenges for both professionals and researchers. Indeed, a primary mission of Risk Managers is to help companies to maximize profit through minimizing the cost of risk (Lei, 2011). The latter being the equilibrium between the cost of risk management and the loss due to their eventual risk realization (Zhang, 2009). Therefore, it is very important to choose and implement the risk management process which is adapted to information system studied context. Hence there is a real need of an information system risk management literature review which is the main of this paper.

Establishing this literature review aims to be aware of various concepts and important approaches related to risk management. The scope of the literature review conducted was as follows. The original set of papers was formed from the searchers run on Elsevier, Science direct, IEEE Xplore and google scholar. The search was constructed from the keywords “Risk”, “information security”, “IS risk management” and “risk management”. This delimiting method based on the use of keywords helps us to find the most relevant papers through linking concepts. The search covered the period between 1990 and 2018. The resulting set of papers undergone manual duplication. Next, papers were selected for review manually based on the examination of the title, abstract and full text. In this paper, we give the outline of the state of the art of the risk management especially in information systems. Some fundamental concepts and model are introduced to interpret the process of IS risk management. We proceed with the description and analysis of the methods. The analysis was done based only on our interpretation of the papers.

This paper is divided into six sections. The second section analyses the concept of risk and risk management in general being a part of risk management activity and its specific meaning in the information system. The third and fourth sections present IS risk / risk management systems. While the fifth section gives a benchmarking according to proposed criteria deduced. Sixth section concludes.

2. Background

2.1 Risk Concept

Risk makes sense in every single human effort (Damodaran, 2008). It had been defined in several ways (Walke, Topkar, & Matekar, 2011). It often carries different technical meanings in different fields and can be used in different cases, this multidisciplinary hamper us from finding some common consent in terms of its definition and utilization. Risk is an important part of individual and organizational decision-making processes and, in many situations, risk taking seems to be the only available strategy to deal with risk (Hora and Klassen, 2013).

The concept of risk varies according to the views, attitudes and experiences of each individual and it is affected by its own mindset (Baloi & Pence, 2003), (Walke, Topkar, & Matekar, 2011). Engineers and designers look at risk from a technological perspective. Others look at it from an economic and financial point of view or from the side of environmental and health (Baloi & Pence, 2003), (Walke, Topkar, & Matekar, 2011).

Table 1. Risk definitions

The Encyclopedia Larousse		Presents the risk according to four visions: (1) possibility, probability of a fact, of an event considered as an evil or damage (2) a more or less probable danger to which one is exposed. (3) Being engaged in an action that could bring an advantage, but that involves at the same time accurate danger. (4) Damage, eventual loss that insurance companies guarantee against the payment of a premium.
Risk compared to probability	(ISO, 2009-b)	"the effect of uncertainty on objectives"
	(IFACI, Price Waterhouse Coopers, & Landwell, 2005)	it represents the "possibility that an event will occur that will have an impact on the achievement of objectives. Risk is measured in terms of consequences and probability. ".
	(Damodaran, 2008)	Some definitions which are given to the risk as a term are based on occurrence of the risk event
	(Shenglan Ma, Hao Wang, Hong-Ning Dai, 2018)	Risk is the combination of the probability of an event and its result.
	(Burtonshaw-Gunn, 2009)	"the threat or possibility that an action or event adversely or positively affects an organization's ability to achieve its objectives".
Risk such Threat (definitions focused on threats and potential causes of risk events)	(Callon, Lascoumes, & Barthe, 2001)	"Risk refers to a well-identified danger that combines the occurrence of one or many events that are perfectly describable, of which we take no heed if they are going to be fulfilled but we know they are likely to happen. ".
	(Liang and al, 2013)	Risk is a measure of the extent to which an object is threatened by a potential event. Many factors can affect the level of risk in different aspects, such as the value of the negative impact on the organization when the circumstance or event occurs, the probability of occurrence of the circumstance or event.
	(Damodaran, 2008)	A third perception considers risks as negative consequences.
Risk as negative results	(Haseeb, Xinhailu, Bib, & Rabbani, 2011)	they consider that the risk is the possibility of suffering a loss and its impact on the party concerned
	(Suroso, J.S., Rahadi, B., 2017)	The risk is the possibility of damage caused by an act. Risk management is a structured approach to managing uncertainties associated with a threat or a range of human activities. The strategies adopted, which involve transferring risk to another party, avoiding risk, reducing the negative effects of risk and taking into account all or part of the consequences of a particular risk.
	(Allen, 1995)	the risk is a composition of four essential parameters, which are the probability of occurrence, the severity of the impact, the sensitivity to change, and the degree of interdependence added to other risk factors.

Risk through the components (risks as formalized interactions between different elements)	(Loosemore, Raftery, & Reilly, 2006)	probability and consequences are two terms employed to express and evaluate risks
	(AlBahar & Crandall, 1990)	function of uncertain events, potential losses or even gains

2.2 Information System as a Work System

There are several definitions of an information system. In our study, we adopted that of the IS as a work system (WS) (Alter, 2008). We opted for this definition since it clearly identifies the components of an IS and eliminates any confusion with the information technology (IT) systems. A work system is a system (Figure 1) in which human participants and/or machines perform work (processes and activities) using the information, technology, and other resources to produce specific products and/or services for of internal or external customers (Alter, 2008).

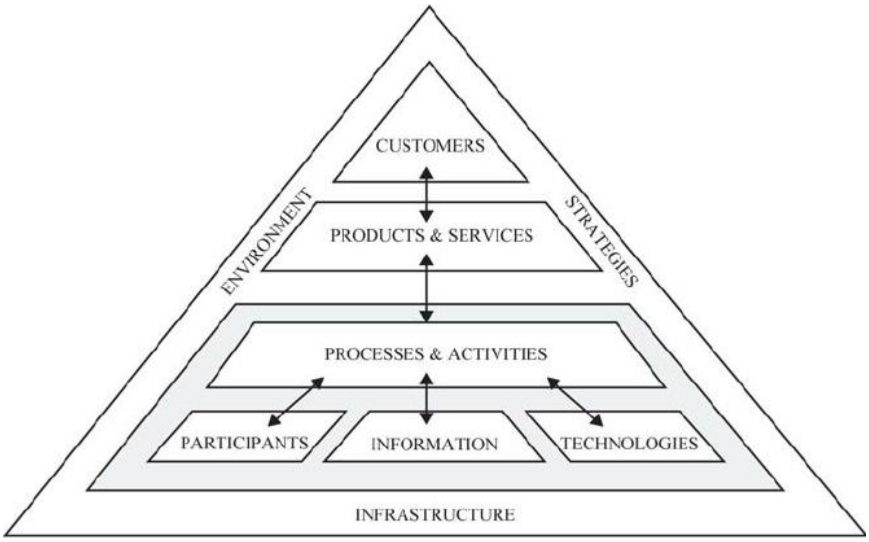

Figure 1. The work system Framework (Alter, 2008)

An information system is a work system whose processes and activities are devoted to processing information, that is, capturing, transmitting, storing, retrieving, manipulating, and displaying information (Alter, 2008).

2.3 Information System Risk

In information systems, the risk concept also lacks precision (Wang, X, Williams, M.A, 2010) and agreement. Previous research related to information systems focuses primarily on development (Goldstein, Benaroch, & Chernobai, 2008) and security risks.

In fact, related to the sphere of information security, several definitions of the concept of risk exist. (Zhang, 2009) for example, states that the risk of the information system is "a probability function that describes the occurrence of the uncertainty event associated to the eventual loss". (Slade, 2006) is based on notions of threat and vulnerability to define risk. He considers that the risk is "the expectation of loss expressed as the probability that a specific threat exploits some vulnerability giving rise to a harmful outcome". In the same vein, (Datta, 2010) defines IS risk as "the impact of achieving a" threat "on a" vulnerability "according to the" risk "equation = Threat x Vulnerability x Cost of the event. Vulnerability being a weakness in any system whose exploitation, intentional or accidental, leads to a violation of the security policy or a negative impact on the asset, as well as any non-compliance with the security requirements of the security information "(Datta, 2010). (BSI, 2010) defines a new notion for grouping the relationship between the three concepts: probability, vulnerability and threat. This is the risk of exposure. It is introduced by the author as "the probability that an element of the system does not have sufficient protection to be able to counter the effects of a threat". It then defines IS risk as a "combination of exposure risk and impact" (BSI, 2010).

(Macedo, 2009) is also interested in IS security. Nevertheless, he attributes a generic definition of the IS risk which involves the probability of negative impact on the results because of: (1) an unadjusted information systems strategy, (2) its ability of adaptation to new requirements and enterprises needs or (3) bad IS security management (Macedo, 2009).

(Mayer N., 2009) offers in the same context a rather interesting definition of IS security risks and its components. It is designed by collecting together all definitions given by standards, and a method that handles IS security risks. (Mayer N., 2009) defines security risk as the "combination of a threat with one or more vulnerabilities that creates a negative impact on one or more assets". Threat and vulnerabilities are sort of the cause of risk and the impact refers to the consequence (Mayer, Heymans, & Matulevicius, 2007).

In such of information management discipline, the risk of information is defined by (Klassen, Borek, Parlikad, & Kern, 2012) as "the effect of the uncertainty of objectives resulting from the poor quality of information ".

In order to propose a risk management model for a special category of information systems, smart IS, (Wang, X, Williams, MA, 2010) consider that an IS risk is a combination of occurrence uncertainty of the possible consequences of an initial event, and their impact, positive or negative, on the intelligent information system in relation with the achievement of its objectives (Wang, X, Williams, MA, 2010).

The framework developed by ISACA, Risk IT, defines IT risk as "the business risk" associated with the use, possession, exploitation, involvement, influence and adoption of IT in every organization (RISK IT, 2010) . (Westerman & Hunter, 2007) define IT risk as "the possibility that an unplanned event, involving failure or misuse, threatens a business purpose". An IT risk incident has the potential to produce substantive business impacts that affect a wide range of stakeholders (Westerman & Hunter, 2007).

(Salvati, 2008), in his work on IS risk management, adopts the definition of ISO applied to the information system: "IS risk is described as the combination of the probability of an event and its consequences ".

(Radut, 2009) considers that IS risk management is "a framework for classifying, assessing and mitigating IS risks up to an acceptable impact". (Olzak, 2008) believes that information risk management is "the appropriate application of business risk mitigation tools and methods leading to the implementation of security controls, the correct use of which mitigate the business risk associated with an information system to a level acceptable to management. This must be done in a way that maintains the highest level of operational efficiency possible for the personnel and processes using the systems protected by these controls. "

While developing his IS security risk model, (Mayer N., 2009) adopts the definition of (ISO, 2009-b). The author considers that IS risk management is "the set of coordinated activities to guide and control an organization in relation to the IS risks to which it is exposed". According to (Florescu Vasile, 2008), IT risk management consists on analyzing the knowledge of the risk taken by the company through its IT systems in terms of business impact.

(Salvati, 2008) believes that beyond the procedural aspects that are often emphasized in the description of IS risk management activities, it is necessary to highlight the decision-making aspects as well (Salvati, 2008). In such interpretation, IS risk management represents a structured approach to risk-informed decision-making which aligns the functioning of the enterprise risk appetite information system (Salvati, 2008). In the same vein, the Risk Management Guide for US Department of Commerce Information Technology Systems argues that information risk management must exist not only to protect its IT assets but also to "protect organization and its ability to fulfill its mission ", (Borek, Parlikad, & Woodall, 2011). Therefore, the risk management process should not be primarily treated as a technical function performed by IT experts who operate and manage the computer system, but as a core management function of the organization (Stoneburner, Goguen, & Feringa, 2002). Information risk management needs to be incorporated into all decisions and day-to-day operations and can be, if used effectively, a tool to manage information proactively rather than reactively.

Given the existing definitions and our understanding of the different aspects of this discipline, we propose the following definition for an IS risk: "an IS risk is any probable event that may occur in its elements and impact the achievement of its objectives".

2.4 Risk Management Discipline

2.4.1 Risk Management Definition

Risk management is “a complex and systematic activity that requires the involvement of entire organization.” (L. Liang, W. Ren, J. Song, 2013). According to (Simister, 2000) the concept of "risk management" (RM) was employed for the first time in insurance companies in the United States during the 1950s. Risk management migrates from a necessity to even an obligation that protect the company assets but also became a regulatory obligation in several cases. Risks can be transferred, managed, minimized or shared, but should never be ignored (Latham, 1994). When faced with a risk, we must act.

In the same way, the risk management discipline has several definitions which don’t express necessarily the true meaning and true scope of this discipline. In fact, (Walke, Topkar, & Matekar, 2011) assert that it is often confused or restricted to one of the four following activities: identification, analysis, and monitoring and / or risk control.

However, other more relevant and more generic definitions exist. Some of them see risk management through the "purpose" view. We call to mind that one proposed by (ISO, 2009-b) standard stating that risk management is "the set of coordinated activities for the purpose of leading and controlling an organization toward risk". (Merna, 1996) defines proportionally this discipline as "the set of actions taken by individuals or companies as an effort to protect their activities from any arising risk ". As for (Merna & Al-Thani, 2005), risk management "aims to obtain, throughout a project life, the optimal or acceptable degree of risk elimination or its control ". This averment concerns project management field but remains valid in a more general context. According to (Flaherty & Maki, 2004) "Enterprise risk management deals with the risks and opportunities that impact the creation or preservation of value".

Other definitions perceive risk management in a more formal and specific way by adopting a systematic process. For example, (Macedo, 2009) considered risk management as a "logical approach to setting the context, analyzing and assessing risks, implementing necessary curative controls, to improve the dedicated system". (Crawford, 2002), thought that risk management aims to identify, analyze, react and control risk factors throughout a project life. The COSO standard considers that risk management is "a process that involves directors, managers, shareholders and even all employees working for an organization. It should go with the development strategy as well as in all other operational activities. It is designed to identify potential events that may affect the organization and manage risks within a tolerance threshold. It aims to provide reasonable assurance to achieve organization objectives"(COSO, 2004). Risk management is defined by COSO as: “a process, effected by an entity’s board of directors, management and other personnel, applied in a strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives”. (COSO, 2004).

Risk management has been developed academically over time from the analysis of an event, its probability and its contribution multiple events analysis (Kumar, 2010). Risk management must also consider both opportunities (possible gains) and threats (potential losses). According to ISO 31000, risk management is coordinated activities to direct and control organization with regard to risk.

2.4.2 Information System Risk Management

According to (Shenglan Ma, Hao Wang, Hong-Ning Dai, 2018), the purpose of risk and information systems is to detect and mitigate all risks appropriately, and to ensure that the organization diminishes risks to an acceptable level. IS risk management definition and characteristics are obviously related to risk management. According to Alter, IS risk management is an ongoing business of identifying and mitigating risks (Alter & Sherer, 2004). IS risk management activities must be included in a realistic model that describes efficiently the overall system of the organization, because the recognition of risk factors encourages appropriate risk reduction tactics (Alter & Sherer, 2004). For example, project managers who do not have an essential skill can use an employee or consultant who do have such ability or completely modify the project skills (Alter & Sherer, 2004) otherwise. The risk reduction tactics available depend on the objectives and expectations that apply (Alter & Sherer, 2004). For example, a project that aims to minimize costs finds additional difficulty in hiring expensive consultants. (Alter & Sherer, 2004).

(Radut, 2009) considers that IS risk management is "a framework for classifying, assessing and mitigating IS risks until achieving an acceptable threshold".

(Olzak, 2008) believes that information risk management is "the proper employment of tools and methods leading to security controls implementation allowing a business risk extenuation and by then insuring information system performance. This must be done in a way that maintains for each personnel and processes, protected by these controls and using the systems, to the highest level of prospective operational efficiency. "

When developing its IS security risk model, (Mayer N., 2009) adopts the definition of (ISO, 2009-b), which considers that IS risk management is "the set of coordinated activities to guide and control an organization in relation to the IS risks to which it is exposed". According to (Florescu Vasile, 2008), IT risk management consists on analyzing the risk knowledge taken by the company through its IT systems in terms of business impact.

For (Saleh, M. S., & Alfantookh, A., 2011), the target ISRM framework is composed of two parts: one concerns its structural view (two dimensions: scope and criteria); while the other is related to its procedural view (two other dimensions: processes and tools). (Shameli-Sendi, A., Aghababaei-Barzegar, R., & Cheriet, M., 2016) proposed a taxonomy for IS risk assessment approaches which is generally classified in four categories: Appraisement, Perspective, Resource Valuation, and Risk Measurement.

(Salvati, 2008) believes that beyond the procedural aspects that are often emphasized in the description of IS risk management activities, it is necessary to highlight the decision-making aspects as well (Salvati, 2008). In such interpretation, IS risk management represents a structured approach to risk-informed decision-making which aligns the functioning of the enterprise information system to its risk appetite (Salvati, 2008). In the same vein, the Risk Management Guide for US Department of Commerce Information Technology Systems argues that information risk management must exist not only to protect its IT assets but also to "protect organization and its ability to fulfill its mission ", (Borek, Parlikad, & Woodall, 2011). Therefore, the risk management process should not be primarily treated as a technical function performed by IT experts who operate and manage the computer system, but as a core management function of the organization (Stoneburner, Goguen, & Feringa, 2002). Information risk management needs to be incorporated into all decisions and everyday operations, can afterwards provided to be used effectively, regarded as tool to manage information proactively rather than reactively.

3. Risk Management System/ Framework/ Process

3.1 Research Works

Risk management is, according to (Woody, C. ,2006), “a repetitive process that addresses the analysis, planning, implementation, control and supervision of the policies and measures of security policy implementation.” In fact, (Hubbard, 2010) risk management process typically contains four steps: (1) risk identification, (2) risk assessment / measurement, (3) risk mitigation options choice and implementation, (4) results monitoring. (Burtonshaw-Gunn, 2009) shares this same decomposition and asserts that all descriptions follow a similar basic approach to identification, quantification, response and risk control. Although the denominations of the four phases may sometimes differ, this classification is adopted by several other authors. Likewise, (Thevendran & Mawdesley, 2004) decompose the risk management process into four phases: identification, analysis, response planning, and risk monitoring and control. In the same way, (Dikmen, Birgonul, Anac, Tah, & Aouad, 2008) define risk management as a procedure consisting of: (1) risk identification; in which uncertainty sources are defined, (2) the risk analysis; it’s about assessing the consequences of uncertain events, (3) the risk response: appropriate strategies based on the expected results statement, and 4) the analysis of the treatment results and the risks that have arisen leads to a possible repetition of the first three stages. According to (Merna & Al-Thani, 2005), risk management has an iterative continuous cycle of identification, analysis, control and reporting.

However, there is some works that propose a different grouping of risk management process activities. For example, (Smith, 2002) defines three processes for risk management: identification, analysis, and response. This grouping neglects surveillance and monitoring phase, which have an important effect as an essential activity in risk management.

As for the Classification proposed by (Crawford, 2002), it defines a fifth component in addition to this classification: the risk documentation. According to (L. Liang, W. Ren, J. Song, 2013), Risk Management Framework (RMF) integrates information security and the management activities into system development life cycle, as described in figure 2 below:

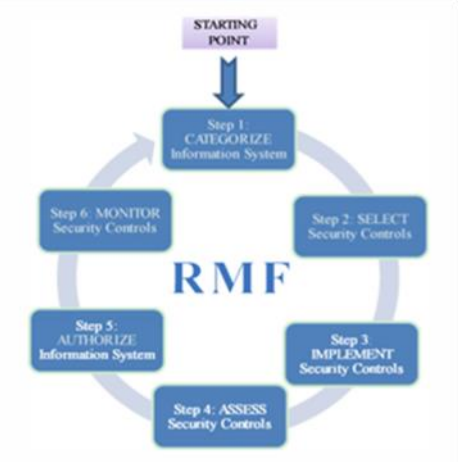
STARTING POINT
Step 1: CATEGORIZE Information System
Step 2: SELECT Security Controls
Step 3: IMPLEMENT Security Controls
Step 4: ASSESS Security Controls
Step 5: AUTHORIZE Information System
Step 6: MONITOR Security Controls
RMF

Figure 2 Risk Management framework (L.Liang, 2013)

As for (Shenglan Ma, Hao Wang, Hong-Ning Dai,2018), they set up a sharing mechanism of risk information among IoT devices, insiders, and information systems based on the risk and information system control framework. They use blockchain technology to make sure that information can be traced.

3.2 Norms and Standards

3.2.1 COSO

According to the COSO standard, risk management is not a sequential process where each element affects only the next. On the contrary, it is a multidirectional and iterative process whereby any element has an immediate and direct influence on the others (COSO, 2004). COSO proposes a risk management system consisting of eight elements (COSO, 2004): (1) the internal environment: encompasses the culture and spirit of the organization, (2) the objectives which must be defined beforehand so that management can identify potential events that could affect its achievement, (3) events: internal and external events that may affect the achievement of an organization's objectives should be identified by distinguishing between threats and opportunities, (4) risk assessment: Risks are analyzed, both in terms of their probability and their impact. The inherent and residual risks are assessed, (5) the treatment of risks: the management defines solutions to face the risks, (6) the control activities: policies and procedures are defined and deployed to ensure the establishment and effective application of risk-management measures, (7) information and communication: useful information is identified, collected and communicated in a format and within a timeframe allowing employees to exercising their responsibilities, and (8) steering: the risk management process is managed in its entirety and modified according to needs. Organizations, in order to achieve their objectives, need to develop interconnected strategies and objectives across the firm. The COSO ERM Framework splits these strategies and objectives into four categories: strategic, operations, reporting and compliance. These categories provide a dimension that creates a strong context for risk consideration.

3.2.2 ISO 31 000

The ISO 31000 standard in its version 2009 provides a structured risk management framework in three parts (Figure 3): (1) risk management principles, (2) organizational risk management framework, and (3) risk management process.

The "Principles" section aims to guarantee the effectiveness of risk management. Eleven principles are proposed: (1) risk management creates value and preserves it, (2) risk management is integrated into organizational processes, (3) risk management is integrated into the decision-making process, (4) risk management deals explicitly with uncertainty, (5) risk management is systematic, structured and used in a timely manner, (6) risk management is based on the best available information, (7) risk management is adapted, (8) Risk management integrates both human and cultural factors, (9) risk management is transparent and participatory, (10) risk management is dynamic, iterative and responsive to change and (11)) risk management facilitates continuous improvement of the organization.

The organizational framework provides the bases and provisions for the risk management integration at all organization levels (ISO, 2009-a). It facilitates effective risk management at different organizational levels and in specific contexts (ISO, 2009-a). It ensures that risk information is properly reported and serves as a basis for decision-making and accountability at all relevant levels within the organization (ISO, 2009-a).

The organizational framework of risk management consists of five components: (1) mandate and commitment, (2) Design of the organizational risk management framework, (3) implementation of risk management, (4) monitoring and organizational framework review and (5) continuous improvement of the organizational framework (ISO, 2009-a).

-Mandate and commitment: serves to formalize management's commitment to support risk management in terms of existence and efficiency.

- Design of the organizational risk management framework: it is done via: (1) the understanding of the organization and its context, (2) the establishment of the risk management policy, (3) the definition of the responsibilities (4) the integration of risk management into organizational processes, (5) resources definition, (6) the establishment of communication and reporting mechanisms and editing either internal reports (7) or external reports (ISO, 2009-a).

- Risk management implementation: this involves: the implementation of (1) the organizational risk management framework, and (2) the risk management process (ISO, 2009-a).

- Monitoring and the organizational framework review: the objective is to ensure the effectiveness of risk management and to contribute to the achievement of performance. It is done through: (1) the performance measurement of risk management using indicators of which relevance is reviewed periodically, (2) the periodic measurement of progress and deviations respecting the risk management plan, (3) periodic review of the organizational framework, risk management plan and policy to ensure that they still concur both the internal and external organization context, (4) reporting risks, the progress of the risk management plan, and how the risk management policy is followed, and (5) the verification of the effectiveness of the organizational risk management framework. (ISO, 2009-a)

- Continuous improvement of the organizational framework: Based on the results of monitoring and reviews, it aims to make decisions about the improvement possibilities for the organizational framework, the risk management policy and plan (ISO, 2009- at).

This framework third component proposed by ISO 31000 is the "risk management process". It is structured in five phases: (1) communication and consultation, (2) context setting, (3) risk assessment, (4) risk management, and (5) monitoring and review.

- Communication and consultation: this phase includes developing as well as circulating a communication plan as soon as the risk management process is created, at each phase and at every update. It must be ensured that it implicates all stakeholders conforming to agreement principle and must be clear and effective.

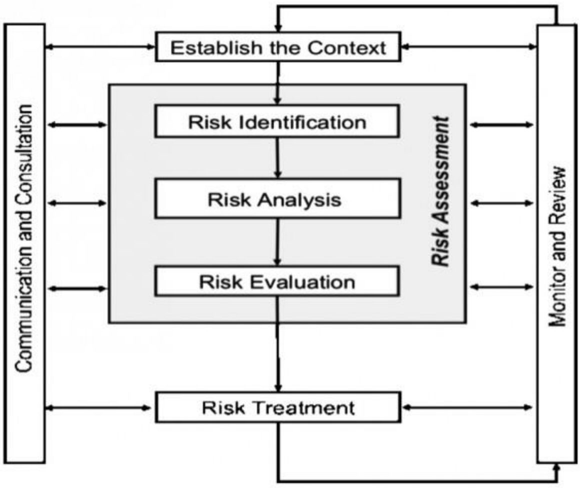

Figure 3. RM framework, ISO 31000

- Setting context: During which one, the organization pinpoints the context where the risk management process has been developed and followed. It clearly specifies its objectives, the internal and external parameters to be a must in risk management, and also ascertains the action sphere and risk criteria for the rest of process.

- Risk assessment: there is talk of identifying, analyzing and evaluating the risk.
- Risk treatment: it shows the methods and the means implemented to control the risks. The treatment stage goes through two operations. The first is comprised of risk treatment options selection follow-on a comparison of implementation costs and efforts with regard to the achieved benefits, taking into account legal, regulatory and other requirements. The second is risk treatment plans development and implementation. These are intended to inform how the chosen treatment options were implemented. The risk treatment involves an iterative process which consists of evaluating what was done, generating new treatments for the residual risks that are intolerable, and subsequently evaluating their effectiveness.
- Monitoring and Review: they are projected and planned in agreement with the organization's context in order to control and improve the risk management process.

The ISO 31000 standard adds a new activity to the risk management process; even if it does not appear in the proposed Framework. It’s precisely about the risk management process registration. The purpose here is to draw the different risk management process activities.

4. Risk Management Processes/ Methods for Information System

In the same way that there are multiple definitions of risk management, there are several works that propose risk management systems in the literature (Schlaak, Dynes, Kolbe, & Schierholz, 2008).

4.1 Softwares Development Risk Management

When studying the relationship between IT and risk management (Radut, 2009) claimed that there are many effective risk management models that can be adopted, depending on the suitability of each firm or the type IS projects implementation. He believes, however, that the risk management process consists primarily of: (1) risks or uncertainties identification, (2) implications analysis, (3) risk response, and (4) distribution on appropriate hazards (Radut, 2009). (Radut, 2009) is also interested in the relationship between the IS risk management and its life cycle. He says that Risk Management can be used effectively and differently for each phase of an IS's development life cycle. He proposes risk management integration in the life cycle. The idea of this approach turns out to be interesting. Nevertheless, the IS as presented through this definition as well as the life cycle remains restricted to software aspects.

4.2 Information Quality Risk Management: TIRM Process

(Borek, Wooaall, Gosaen, & Parlikad, 2011) are interested in the management of information quality risks by proposing the Total Information Risk Management (TIRM) process. Its goal is to develop effective initiatives for improving the quality of information (Borek, Wooaall, Gosaen, & Parlikad, 2011). TIRM is a systematic and holistic approach based on formal risk assessment and management and is concerned with the concept of global risk management (Haimes, 1991). It aims to manage risks arising from potential information resources, all types combined including information resulting of databases, documents, humans, and external and internal environment, both tacit and explicit, structured and unstructured, etc. (Borek, Parlikad, & Woodall, 2011). The TIRM process is based on the ISO 31000 risk management standard (ISO, 2009). It uses the matched framework but fits the risk management process to the practices of the quality of information discipline (Borek, Parlikad, & Woodall, 2011). It is divided into five activities: (1) communication and consultation, (2) context setting, (3) information risk assessment, (4) information risk treatment, and (5) monitoring and review.

4.3 Security Information Risk Management

(Khoo B, Harris P, Hartman S, 2010) Information security can be defined as “the protection of the confidentiality, integrity and availability of information and its critical elements, including th software and hardware that use, store, process and transmit that information through the application of pilic, technology, education and awareness”

Several studies are led in IS security risk management. These works are formalized in terms of methods, standards and research work.

Traditional risk management methods related to information systems security are no longer adapted to the complexity of organizations and the associated risks in such a context of compliance and governance. Because of these problems, new solutions are needed to deal with security risks (Mayer N., Aubert J. 2018).

4.3.1 Information Security Risk Management Generic Process

According to (Mayer N., 2009) a generic process followed by SI security risk management methods consists of six steps (Figure 4).

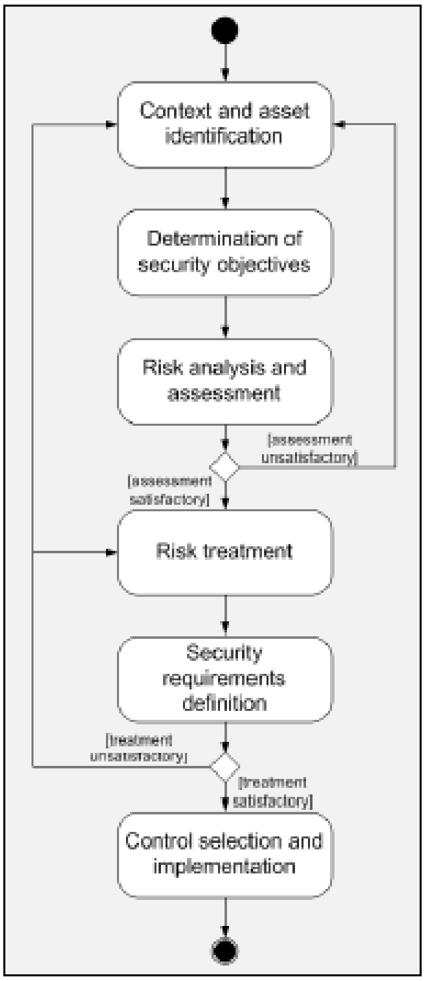
Context and asset identification
Determination of security objectives
Risk analysis and assessment
[assessment unsatisfactory]
[assessment satisfactory]
Risk treatment
Security requirements definition
[treatment unsatisfactory]
[treatment satisfactory]
Control selection and implementation

Figure 4. Information security risk management generic process (Mayer N, 2009)

These steps are (Mayer, Heymans, & Matulevicius, 2007): (1) the context study and identification of the organization assets. In this step, the organization and its environment are presented. An overview of the information system is also established, (2) the security objectives determination in line with the protection level required for the assets. These objectives are often defined conforming to three criteria: confidentiality, integrity and availability, (3) risk assessment: it determines which threats can harm assets and threaten security objectives. It consists of identifying the risks and assessing their level in a qualitative or quantitative way. The assessment is made following a comparison between the level of the analyzed threats and the security needs already defined, (4) risk treatment: once the risk analysis has been carried out, the decisions concerning the treatment of the risks are taken and (5) Determination of security requirements that are determined as security solutions to mitigate risks, and (6) implementation of security control requirements.

4.3.2 Information Security Risk Management Methods

Octave (Operationally Critical Threat, Assets, and Vulnerability Evaluation) was created by the University of Carnegie Mellon (USA) in 1999. Octave is intended for large companies, but recently a version adapted to small structures exists: Octave- S. Its purpose is to enable a company to carry out risk analysis of its IS by itself, without outside help (consultants).

Octave is composed of 3 phases:

- organizational view

- technical view
- security strategy

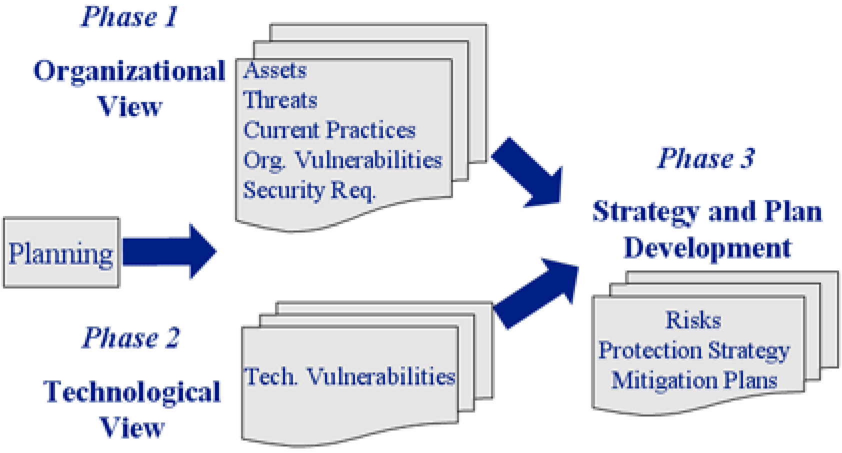

Figure 5. Octave phases

The following three phases are at the heart of OCTAVE, respect the progressive analysis of the three blocks of risk management concepts.

• Phase 1 (Organizational View) provides control over resources, associated threats and threats. the security requirements that are associated with them. It identifies the company's assets, the threats to its operation, the vulnerabilities of its organization, the security objectives imposed by management, and the current security measures. These are three information gathering processes that are carried out during this phase, each by a particular population: senior managers, operational managers and production teams. Consolidating information from these processes leads to creating threat profiles.

• Phase 2 (technical view) identifies vulnerabilities in the infrastructure. Thisview identifies the essential elements of each asset identified above and audits them for vulnerabilities.

• Phase 3 of the development of the security strategy consists of evaluating the identified risks (impact, probability) above and proposing measures to reduce them. A risk reduction plan is then planned.

The simplicity of the Octave method makes it in principle an effective method, it is quite common in the United States and Quebec. It focuses on the protection of company assets and the management of personnel. It covers all of the company's business processes at all levels (organizational and technical).

This method involves the creation of a multidisciplinary team comprising members of all departments of the company. It will enable them to improve their knowledge of their company and to share good security practices.

We also find in this method all the concepts required in the first part. Regarding the process, the same-made for EBIOS, are available: the last two steps, are one way to be, are method of a self-risk decisions.

CRAMM (CCTA Risk Analysis and Management Method) was invented by Siemens in England and is supported by the state. Cramm is a fairly extensive and exhaustive method for large companies, as it uses nearly 3,000 checkpoints. It has two variants: Cramm Express and Cramm Expert and is compatible with BS7799.

The Cramm method is composed of 3 phases:

- identification of the existing
- assessment of threats and vulnerabilities
- choice of remedies

The identification of the existing one makes it possible to draw up an inventory of the equipment, the applications, and the data which constitute the IT infrastructure on which the IS of the company is based. Each element of this inventory is evaluated in terms of cost and impact in case of compromise (unavailability, alteration, destruction ...).

The assessment of threats and vulnerabilities highlights possible problems. For this, Cramm's knowledge base provides an important list of possible risks whose criticality level must be assessed.

The choice of remedies consists in selecting among a base of 3,000 possible countermeasures classified in 70 themes the remedies to the risks identified above. The software provided with Cramm determines the remedies to be adopted according to the risks, their previously identified criticality and the desired level of security.

Mehari (Harmonized Method of RIsque Analysis) has been developed by CLUSIF since 1995 and is derived from the Melisa and Marion methods. Existing in French and English, it is used by many public companies as well as by the private sector.

Mehari's general approach consists in analyzing security issues: what are the feared scenarios? and in the prior classification of IS entities according to three basic security criteria (confidentiality, integrity, availability). These issues express the dysfunctions that have a direct impact on the company's activity. Then, audits identify the vulnerabilities of the IS. And finally, the actual risk analysis is done.

4.3.3 ISO 27005 Standard

The ISO 27005 standard, unlike other standards in risk management, allows to build results that evolve with the organization. Any minor or major change can be incorporated into the risk management process. The ISO 27005 standard (ISO, 2011) provides an approach for setting up a risk management system but only in the context of information security. It proposes a methodology in compliance with ISO / IEC 27001 and which applies the PDCA improvement cycle (Plan, Do, Check, Act). The risk management process consists on six phases (Figure 6): (1) Context Setting: Defines the risk management fields, boundaries and environment process. During this phase, the risk management criteria are established: the treatment thresholds for the evaluation, the thresholds for taking into account the risks with respect to their impact and the acceptance thresholds, (2) assessment of the risks. risks: The first step of this phase is to define the context and the elements that compose it such as the organization, the information system, the essential elements to protect, the entities that depend on it and the various constraints that may arise. Then, it is necessary to express the security needs of the essential elements, to identify and characterize in terms of opportunities the threats weighing on the information system. Finally, risks are determined by confronting threats to security needs. These risks are analyzed and evaluated in order to set priorities and schedule them according to their evaluation criteria, (3) Risk treatment: This is the process of selecting and implementing security measures. This begins with identifying security objectives which constitute the specifications of the risk treatment process. Then, security requirements are determined to meet the security objectives and to describe how to address the risks. To define treatment options, the risk and cost of treatment must be matched, (4) risk acceptance: This is a safety accreditation performed by a designated probate authority for a specified period of time. This approval requires a security file examination whose content must be defined. (5) Risk communication: This is an exchange and a regular sharing of information on risks between the risks manager, decision makers and all stakeholders. This risk communication helps to: (a) reduce misunderstandings with decision-makers, (b) gain new knowledge in safety, (c) involving the responsibility of decision-makers. The last phase is: (6) monitoring and risk review to ensure that the process remains relevant and adapted to safety objectives. It is also necessary to identify the changes requiring a risk reassessment as well as the new threats and vulnerabilities.

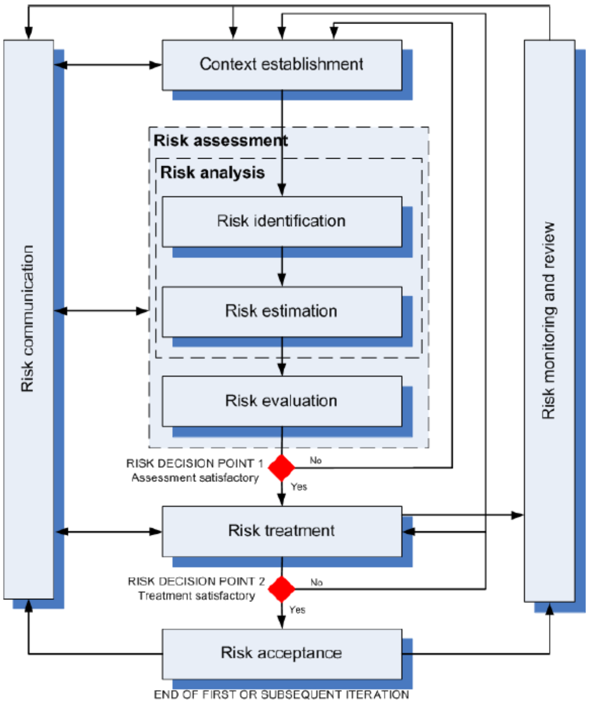

Figure 6. Processus 27005 de gestion des risques de sécurité SI (ISO, 2011)

4.3.4 IT Risk Management: Risk IT

IT Risk defines best practices in IT risk management by providing a framework for businesses to identify, govern and manage information technology (IT) risks. (Shenglan Ma, Hao Wang, Hong-Ning Dai,2018) IT risk management refers to the execution of risk strategies that reveal the organization's preferences, culture, and management tolerances, takes into account technology and budgets, while meeting regulatory requirements and conformity.

(Cherdantseva, Burnap, 2016) propose a classification of cybersecurity risk assessment methods for SCADA systems. They divide the methods examined into elaborate guidelines, activity-specific methods and guidelines. They then classify the methods into categories according to a model and a formula.

The IT Risk Framework comprises three areas: (1) Risk Governance (RG), (2) Risk Assessment (ER) and (3) Risk Response (RR).

The goal of the RG domain is to ensure that IT risk management practices are incorporated into the business, that security is optimal and that risks are adjusted (Lapointe, 2010). This area is composed of three processes: (1) RG1: Establish and maintain a common risk view; (2) RG2: Integrate with ERM (Enterprise Risk Management) and (3) RG3: Make decisions on business risks. Each of these processes is split into a set of activities.

The objective of the "Risk Assessment" area is to ensure that IT risks and opportunities are identified, analyzed and considered in business decisions. The processes in this area are: (1) RE1: Gather Data, (2) RE2: Analyze Risks, and (3) RE3: Maintain a Risk Profile.

The objective of the "Risk Response" area is to ensure that IT risks, opportunities, and events are addressed cost-effectively and in line with business priorities. This domain is composed of three processes: (1) RR1: Articulate risks, (2) RR2: Manage risks and (3) RR3: React to events.

IT Risk identifies three types of risks (Stachtchenko, 2009): (1) Provision of IT services. This risk is associated with the IT services performance and availability that can lead to loss or impairment (Service interruptions, security issues, compliance issues, etc.), (2) IT solutions Provision and realization of the benefits associated with the IS contribution to new business solutions or improved solutions in the form of programs and projects (Quality of projects, Relevance of projects, Exceedments, ...), (3) Realization of benefits associated with missed opportunities for use technology to improve the efficiency and effectiveness of business processes or leverage new business initiatives (Stachtchenko, 2009).

5. Comparative Analysis and Discussion

In this section, we led a comparative study of the risk management processes, methods and standards presented above to analyse which of them can be used for information system risk managemen and in which context and area it is more effective. This study is based on the following criteria:

Criterion 1: Completeness of Risk Management Activities: This criterion is based on the requirements that must be met by a risk management process (Hillson, 2010). These requirements are: (1) Process initiation, (2) Risk identification, (3) Priorities identification (risk evaluation), (4) Risk response planification, (5) Risk response implementation, (6) Communication, (7) Risk review and (8) learned lessons.

Table 2 gives the mapping between the presented process/methode/standard and those requirements.

Table 2. Requirement mapping

	Process initiation	Identification	Priorities	response	Implementation	Communication	Risk review	learned lessons
(Burtonshaw-Gunn, 2009)		Identification	Quantification	Risk Responses			Control	
(Thevendran & Mawdesley, 2004)		Identification	Risk Analysis	Responses Planification			monitoring and control	
(Dikmen, Birgonul, Anac, Tah, & Aouad, 2008)		Identification	Risk Analysis	Risk Responses				
(Merna & Al-Thani, 2005)		Identification	Risk Analysis			Reporting	Control	
(Smith, 2002)		Identification	Risk Analysis	Risk Responses				
(Chapman & Ward, 1997)	Define, Focus	Identify	structure, appropriate, evaluate	Responses Plan				
(Crawford, 2002)	Define the context	Identify the risks	Evaluate	Treat		Document		
(COSO,2004)	interne Environment/ objectives definition	Events Identification	Risk evaluation	Risk treatment		Information/ communication	Control/Pilotage	
(ISO, 2009-a)	Establishment of Context	Risk appreciation		Risk treatment		Communication and consultation	Monitoring and review	Recording
(Borek, Parlikad, Woodall, 2011)	Establishment of Context	Risk appreciation	Risk appreciation	Information Risk treatment		Communication and consultation	Monitoring and review	
(Mayer N. , 2009)	Context	Assets/object	Risk	Risk treatment				

	study	ives identification	appreciation	Security requirement definition			
ISO 27005	Establishment of Context	Risk appreciation	Risk appreciation	Information Risk treatment	Communication	Monitoring and review	
Ebios		Identification	Analysis/ evaluation	treatment	Communication		
Cramm		Identification	Analysis/ evaluation				
Octave		Identification	Analysis/ evaluation	treatment	Communication		
Mehari		Identification	Analysis/ evaluation	treatment			

Criterion 2: Integration of IS Risk Management in the overall management of the organization: This integration can be expressed by the following objectives: (1) Ensure that risk management activities create value for the IS studied and therefore for the organization, (2) Integrate IS risk management into a realistic risk management model related to the overall system of the organization, (3) Align the information system operation with the risk appetite of the organism.

Criterion 3: Risk Management Support for All IS Aspects: It is important that the proposed risk management activities are generic enough to ensure the risk management of an IS such as a socio-technical system and more particularly a work system and not only as a technical or computer system.

Criterion 4: Use of Standard Vocabulary: It is important that the chosen process uses a standard risk management vocabulary that is easily understood by the users of the model designed. Table 3 presents the results of this study.

Table 3. Comparative analysis between RM process

Dispositif / RM process	Completeness of Risk Management Activities	Integration of IS Risk Management in the overall management of the organization	Risk Management Support for All IS Aspects	Use of Standard Vocabulary
(Burtonshaw-Gunn, 2009)	5/8	NS	General	NS
(Radut, 2009)	4/8	NS	Software development	NS
(Thevendran & Mawdesley, 2004)	4/8	NS	General	NS
(Dikmen, Birgonul, Anac, Tah, & Aouad, 2008)	4/8	NS	General	NS
(Merna & Al-Thani, 2005)	4/8	NS	General	NS
(Smith, 2002)	4/8	NS	General	NS
(Crawford, 2002)	6/8	NS	General	NS
(COSO, 2004)	7/8	Yes	General	NS
(ISO, 2009-a)	8/8	Yes	General	Yes

(Borek, Parlikad, & Woodall, 2011)	7/8	NS	Information quality	NS
(Mayer N. , 2009)	4/8	Yes	IS security	Yes
(ISO, 2011)	7/8	Yes	IS security	Yes
(ISACA, 2010) (Risk IT)	7/8	Yes	IT risk	NS
EBIOS	4/8	Yes	IS security	No
Cramm	4/8	No	IS security	No
Octave	4/8	No	IS security	No
Mehari	4/8	No	IS security	No

With:

- NS: Not specified.

- In criterion 1:" Completeness of Risk Management Activities", n in ratio n / 8 represents the number of risk management process requirments verified among the 8.

The study shows that ISO 31000 is the one that meets the above criteria better.

In fact, compared to criterion 1, the mapping presented in table 3 between the selected requirements and the activities of the different risk management processes shows that the process proposed by ISO 31000 is the only one that covers all of these requirements.

The ISO 31000 standard through the two components of its Framework: "principles" and "organizational framework", verifies the elements of criterion 2. Indeed, the first two principles of risk management in this standard: "(1) management risk creates and preserves value "and" (2) risk management is integrated into organizational processes "guarantee the first two objectives of this criterion. The organizational risk management framework allows risk management to be organized in such a way as to ensure consistent consistency. IT risk management can only be done within an overall risk management framework of the organization and in accordance with the risk appetite of the organization.

As for criterion 3, the generic aspect of the ISO 31000 risk management process allows it to be applicable to all types of systems and in particular the IS as a work system with all its elements. The device proposed by ISO 31000 also verifies criterion 4. Indeed, it incorporates the notions defined by (ISO, 2009-b) in order to standardize the vocabulary around risk. It is also based on the "AS / NZS 4360" standard, which is proven by industrial reality (Sienou, 2009).

Nevertheless, for specific IS risks, it is important to consider the specificities of risk security processes and methods like ISO27005 and EBIOS.

6. Conclusion

In this paper, we present an overview about the risk management (RM) of information systems (IS). Some fundamental concepts and models are introduced to understand IS risk management. As the information system is a socio-technical system, the study of risk is necessary to ensure the relevance of this paper.

This review focused on the concepts of risk and risk management in general, then those specific to information system. According to this state of art, although the literature is quite rich in this area, there is still no consensus on risk management and IS risk management concepts.

This review introduced the most important risk management and risk management processes for information systems. Then, it shows a comparative analysis of these processes. This analysis shows the applicability of ISO 31000 on risk management of information system as a socio-technical system, but also the need of integration of some RM process specifities when the IS area is specific such as security IS and quality IS. Hence the importance of designing an adaptable IS RM system.

References

AlBahar, J. F., & Crandall, K. C. (1990). Systematic Risk Management Approach for Construction Projects. *Journal of Construction Engineering and Management, 116*(3), 533-546. https://doi.org/10.1061/(ASCE)0733-9364(1990)116:3(533)

Allen, D. E. (1995). Risk Management in Business. MCB University Press.

Alter, S. (1999, March). A general, yet useful theory of information systems. *Communications of the Association for Information Systems (AIS), 1*(13), 1-70. https://doi.org/10.17705/1CAIS.00113

Alter, S. (2002). The Work System Method for Understanding Information Systems and Information System Research. *Communications of the AIS, 9*(6), 90-104. https://doi.org/10.17705/1CAIS.00906

Alter, S. (2006). The Work System Method: Connecting People, Processes, And It for Business Results. Work System Press.

Alter, S. (2008). Defining information systems as work systems: implications for the IS field. *European Journal of Information Systems (EJIS), 17*(5), 448-469. https://doi.org/10.1057/ejis.2008.37

Alter, S. (2010-a). Viewing Systems as Services: A Fresh Approach in the IS Field. *Communications of the Association for Information Systems (AIS), 26*(1), 195-224. https://doi.org/10.17705/1CAIS.02611

Alter, S. (2010-b). Work System Theory: An Integrated, Evolving Body of Assumptions, Concepts, Frameworks, and Principles for Analyzing and Designing Systems in Organizations. Proceedings of JAIS Theory Development Workshop. AIS.

Alter, S., & Sherer, S. A. (2004). A General, but Readily Adaptable Model of Information System Risk. *Communications of the Association for Information Systems (ACM), 14,* 1-28. https://doi.org/10.17705/1CAIS.01401

ANSSI. (2010, Avril). EBIOS 2010 - Expression des Besoins et Identification des Objectifs de Sécurité url : http://www.ssi.gouv.fr/site_article173.htm

Baloi, D., & Pence, A. D. (2003). Modeling global risk factors affecting construction cost performance. *International Journal of Project Management, 21*, 67-76. https://doi.org/0.1016/S0263-7863(02)00017-0

Borek, A., Parlikad, A. K., & Woodall, P. (2011). Towards A Process For Total Information Risk Management (TIRM). Proceedings of the 16th International Conference on Information Quality. Adelaide, Australia.

Borek, A., Wooaall, P., Gosaen, M., & Parlikad, A. K. (2011). Managing information risks in asset management Experiences from an in-depth case study in the utility industry. Asset Management Conference 2011, IET and IAM, (pp. 1-6). London. https://doi.org/10.1049/cp.2011.0551

BSI, B. S. (2010). Information Security Risk Management: Handbook for ISO/IEC 27001. British Standards Institution. https://doi.org/10.1108/09565691111186911

Burtonshaw-Gunn, S. A. (2009). Risk and Financial Management in Construction. Gower. https://doi.org/10.4324/9781315244112

Callon, M., Lascoumes, P., & Barthe, Y. (2001). Agir dans un monde incertain : Essai sur la démocratie technique. Paris : Editions du Seuil. https://doi.org/10.7202/000506ar

Cherdantseva, Y., Burnap, P., Blyth, A., Eden, P., Jones, K., Soulsby, H., & Stoddart, K. (2016). A review of cyber security risk assessment methods for SCADA systems. *Computers & Security, 56,* 1–27. https://doi.org/10.1016/j.cose.2015.09.009

COSO. (2004). The Committee of Sponsoring Organizations of the Treadway Commission - Enterprise Risk Management - Integrated Framework - Executive Summary. New York: AICPA.

Crawford, J. K. (2002). Project Management Maturity Model: Providing a Proven Path to Project Management Exellence. Marcel Dekker.

Damodaran, A. (2008). Strategic Risk Taking: A Framework for Risk Management. Philadelphie, USA: Wharton School Publishing.

Datta, S. P. (2010). Risk Management Process for Information Security System. *International Journal of Computer Science andCommunication, 1*(1), 33-38.

Dikmen, I., Birgonul, M., Anac, C., Tah, J. H., & Aouad, G. (2008). Learning from risks: A tool for post-project risk assessment. *Automation in Construction, 18*(1), 42-50. https://doi.org/ 10.1016/j.autcon.2008.04.008

Eroglu, S., & Cakmak, T. (2016), Entreprise information systems within the context of information security: a risk assessment for a health organization in Turkey, Conference on entreprise information systems/ international on project management/ conference on health and social care Information systems and technologies, CENTERIS/ProjMAN/ HCist 2016, October 5-7,2016. https://doi.org/

0.1016/j.procs.2016.09.262

Flaherty, J., & Maki, T. (2004). Enterprise Risk Management. Integrated Framework: Executive Summary. Committee of Sponsoring Organizations of the Treadway Commission. Retrieved from https://www.coso.org/Documents/COSO-ERM-Executive-Summary.pdf

Florescu Vasile, D. V. (2008). Problématique de la gouvernance du système d'information. *Economic Science Series, 17*(4), 1381-1386.

Goldstein, J., Benaroch, M., & Chernobai, A. (2008). IS-Related Operational Risk: An Exploratory Analysis. Proceedings of the Fourteenth Americas Conference on Information Systems (AMCIS). Toronto, Canada.

Haimes, Y. Y. (1991). Total Risk Management. *Risk Analysis, 11*(2), 169-171. https://doi.org/10.1111/j.1539-6924.1991.tb00589.x

Haseeb, M., Xinhailu, P., Bib, A., & Rabbani, W. (2011). HAZARD RISK ANALYSIS AND MANAGEMENT IN CONSTRUCTION SECTOR OF PAKISTAN. *International Journal of Economics and Research, 2*(04), 35-42. Retrieved from http://ijeronline.com/documents/volumes/Vol2%20issue%204/ijer20110204(5).pdf

Hillson, D. A. (2010). Le Processus Risque de Base. RISK DOCTOR NOTE D'INFORMATION. Retrieved from www.risk-doctor.com/pdf-briefings/risk-doctor54f.pdf

Hora, M., & Klassen, R. D. (2013). Learning from others'misfortune: factors influencing knowledge acquisition to reduce operational risk. *J. Oper. Manag, 31*(1), 52–61. https://doi.org/10.1016/j.jom.2012.06.004

Hubbard, D. W. (2010). How to Measure Anything: Finding the Value of Intangibles in Business. Wiley.

IFACI, PriceWaterhouseCoopers, & Landwell. (2005). Le management des risques de l'entreprise Cadre de Référence. Techniques d'application. Editions d'Organisation.

ISACA. (2010). RISK IT Framework.

ISO. (2009-a). ISO 31000:2009 Risk Management. Principles and Guidelines on Implementation. Tech. rep.

ISO. (2009-b). ISO Guide 73:2009 - Risk management -- Vocabulary. ISO Guide 73:2009 - Risk management -- Vocabulary.

ISO. (2011). ISO/IEC 27005:2011 Information technology -- Security techniques -- Information security risk management. ISO/IEC 27005:2011 Information technology -- Security techniques -- Information security risk management.

Khoo, B., Harris, P., & Hartman, S. (2010), Information security governance of entreprise information systems: an approach to legislative compliant. Information Journal of management and information system, September 2010. https://doi.org/10.19030/ijmis.v14i3.840

Klassen, V., Borek, A., Parlikad, A. K., & Kern, R. (2012). Quantifiying the Business Impact of Information Quality - a Risk-Based Approach. 20th European Conference on Information Systems (ECIS). Barcelone.

Kumar, M. (2010). Risk Management Practices in Global Manufacturing Investment. Cambridge: University of Cambridge.

Liang, L., Ren, W., & Song, J. (2013). The state of the art of risk assessment and management for information systems. 9th International Conference on Information Assurance and Security (IAS). https://doi.org/10.1109/ISIAS.2013.6947735

Lapointe, M. (2010). Survol de Risk IT. Un nouveau référentiel de gestion des risques TI. Journée thématique surles risques. Québec.

Latham, M. (1994). Constructing the Team: Joint Review of Procurement and Contractual Arrangements in the UK Construction Industry. London: HMSO.

Lei, Y. (2011). Minimizing the Cost of Risk with Simulation Optimization Technique. *Risk Management and Insurance Review, 14*(1), 121-144. https://doi.org/10.1111/j.1540-6296.2010.01193.x

Loosemore, M., Raftery, J., & Reilly, C. (2006). Risk Management in Projects. Oxon: Taylor & Francis.

Lupper (2008, 2010). Gestion des risques en sécurité de l'information, Mise en œuvre de la norme ISO 27005. Groupe Eyrolles

Macedo, F. N. (2009, november). Models for Assessing Information Security Risk. Lisbonne: Technical University of Lisbonne.

Mayer, J., & Fagundes, L. L. (2009). A Model to Assess the Maturity Level of the Risk Management Process in Information Security. 4rd IFIP/IEEE International Workshop on BDIM. New York. https://doi.org/10.1109/INMW.2009.5195935

Mayer, N. (2009, April). Model-based Management of Information System Security Risk. Ph.D. Thesis, University of Namur, Namur.

Mayer, N., Aubert, J., Grandry, E., Feltus, C., Goettelmann, E., & Wieringa, R. (2018). An integrated conceptual model for information system security risk management supported by enterprise architecture management. Software & Systems Modeling.McKeen, J., & Smith, H. (2003). Making IT Happen: Critical Issues in IT Management. Wiley. https://doi.org/10.1007/s10270-018-0661-x

Mayer, N., Heymans, P., & Matulevicius, R. (2007). Design of a Modelling Language for Information System Security Risk Management. Proceeding of the 1st international conference on research challenges in information science (RCIS'07) (pp. 121-132). Ouarzazate, Morocco: IEEE Xplore Digital Library.

Mayer, N., & Humbert, J. P. (2006). La gestion des risques pour les systèmes d'information, le magasine MISC n°24 (Avril-Mai 2006), ISSN: 1631-9036.

Merna, T. (1996). Projects Procured by Privately Financed Concession Contracts. Asia Law\& Practice Limited.

Merna, T., & Al-Thani, F. (2005). Corporate Risk Management: An Organisational Perspective. Wiley.

Olzak, T. (2008). A Practical Approach to Managing Information System Risk. Kindle Edition.

Organ, J., & Stapleton, L. (2007). Information Systems Risk Through a Socio-Technical Lens: Future Directions in Systems Risk Research. https://doi.org/10.3182/20120611-3-IE-4029.00027

Radut, C. (2009, May). The Enterprise Information System and Risk Management. *Annals of Faculty of Economics, 4*(1), 1030-1034.

Saleh, M. S., & Alfantookh, A. (2011). A new comprehensive framework for enterprise information security risk management. *Applied Computing and Informatics, 9*(2), 107–118. https://doi.org/10.1016/j.aci.2011.05.002

Salvati, D. (2008). Management of Information System Risks. Zurich: University of Zurich.

Schlaak, B., Dynes, S., Kolbe, L. M., & Schierholz, R. (2008). Managing of Information Systems Risks in Extended Enterprises: The Case of Outsourcing. Proceedings of the Fourteenth Americas Conference on Information Systems (AMCIS) (p. 280). Toronto, Canada : AMCIS.

Shameli-Sendi, A., Aghababaei-Barzegar, R., & Cheriet, M. (2016). Taxonomy of information security risk assessment (ISRA). *Computers & Security, 57,* 14–30. https://doi.org/10.1016/j.cose.2015.11.001

Shenglan Ma, Wang Hao, & Hong-Ning Dai and al. (2018). A Blockchain-Based Risk and Information System Control Framework. IEEE 16th Intl Conf on Dependable, Autonomic and Secure Computing, 16th Intl Conf on Pervasive Intelligence and Computing, 4th Intl Conf on Big Data Intelligence and Computing and Cyber Science and Technology Congress. https://doi.org/10.1109/DASC/PiCom/DataCom/CyberSciTec.2018.00031

Sienou, A. (2009). Proposition d'un cadre méthodologique pour le management intégré des risques et des processus d'entreprise. Thèse doctotale, Institut National Polytechnique de Toulouse, Toulouse.

Simister, T. (2000). Risk management: the need to set standards. *Balance Sheet*, *8*(4), 9-10. https://doi.org/10.1108/09657960010373400

Slade, R. (2006). Dictionary of Information Security. Elsevier Science.

Stachtchenko, P. (2009). Un cadre de référence intégré Val IT, CobiT, Risk IT. IGSI Symposium 2009-Les systèmes d'information et les risques d'entreprises.

Stoneburner, G., Goguen, A., & Feringa, A. (2002). NIST Special Publication 800-30: Risk Management Guide for Information Technology Systems. Gaithersburg: National Institute of Standards and Technology.

Suroso, J. S, & Fakhrozi, M. A. (2018). Assessment of Information System Risk Management with Octave Allegro at Education Institution, 3rd International Conference on Computer Science and Computational Intelligence 2018. https://doi.org/10.1016/j.procs.2018.08.167

Suroso, J. S., Rahadi, B. (2017). Development of IT Risk Management Framework Using COBIT 4.1, Implementation In IT Governance For Support Business Strategy. ACM International Conference Proceeding Series. Part F130654, pp. 92-96. https://doi.org/10.1145/3124116.3124134

Thevendran, V., & Mawdesley, M. (2004). Perception of human risk factors in construction projects: an exploratory study. *International Journal of Project Management, 22*(2), 131-137. https://doi.org/10.1016/S0263-7863(03)00063-2

Walke, R. C., Topkar, V., & Matekar, N. U. (2011). An approach to risk quantification in construction projects. *International Journal of Engineering Science and Technology, 3*(9), 6846-6855.

Westerman, G., & Hunter, R. (2007). It Risk: Turning Business Threats Into Competitive Advantage. Harvard Business School Press.

Woody, C. (2006). Applying OCTAVE: Practitioners Report. Carnegie Mellon University.

Zhang, Y. (2009). A Study on Risk Cost Management. *International Journal of Business and Management, 4*(5), 145-148. https://doi.org/10.5539/ijbm.v4n5p145

Copyrights