Computer and Information Science; Vol. 12, No. 1; 2019
ISSN 1913-8989 E-ISSN 1913-8997
Published by Canadian Center of Science and Education

A Maturity Model for Assessing IS Risk Management Activity Considering the Dependencies Between Its Elements

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

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

[2] ITQAN Team, 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: December 13, 2018 Accepted: January 2, 2019 Online Published: January 26, 2019
doi:10.5539/cis. v12n1p98 URL: https://doi.org/10.5539/cis.v12n1p98

Abstract

The information systems (IS) are a key asset for organizations. Therefore, managing IS risks becomes more and more important especially within a world in perpetual change. Since IS risk management creates added-value, it must follow a process of continuous improvement orchestrated by a maturity model that figures out available pathways for a better improvement. The studied literature shows the lack of an IS risk management maturity model that considers all IS components and specificities of risk management activity. The present article shows first this lack in the section related to the comparative analysis of the existing models. Then, it proposes a maturity model to address this issue. The proposed model aims to assess the information system risk management activity while considering the dependencies between its elements.

Keywords: information system, maturity, maturity model, risk management

1. Introduction

An effective governance of a company needs, inevitably, good governance of its information system because it manages its most important asset: Information. Indeed, the information system (IS) is a set of human resources (personnel), material (equipment) and procedures, which allow acquiring, store, process and disseminating relevant information for the operation of a business or organization (DeCourcy, 1992).

The governance of an information system is the definition and the implementation of the strategy and the necessary tools for the achievement of its objectives. However, those objectives can be achieved only if the IS is protected against any potential threats through the implementation of an effective risk management (RM) process. Thereby, a first question arises: how to measure the effectiveness of this process? Monitoring and review activity, measures the effectiveness of the RM process at the other process activities but in a more corrective than preventive way and in terms of deliverable (risk mapping, treatment...) and not approach. Hence the need of a maturity model for IS risk management process.

Maturity models are significant tools to ensure continuous improvement of systems and activities. They allow self-assessment and provide a relevant benchmark of these activities in relation to best practices (Elmaallam & Kriouile, 2013). However, to be effective they should be relevant and deal with the real issue of the targeted assessement. The second question is then: which maturity model best meets the requirements for information system risk management assessment specially the dependencies between its elements?

In this paper we propose an information system risk management maturity model. The remainder of this paper is structured as follows: Section gives the background of this research. It defines the information system as a work system, describes the existing maturity model architectures with a focus on Focus Area model, lists the existing information system risk management maturity models and evaluates them. Section three presents the proposed model. Section four concludes.

2. Background

2.1 Information System as a Work System

There are several definitions of an information system (Carvalho, 2000). 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).

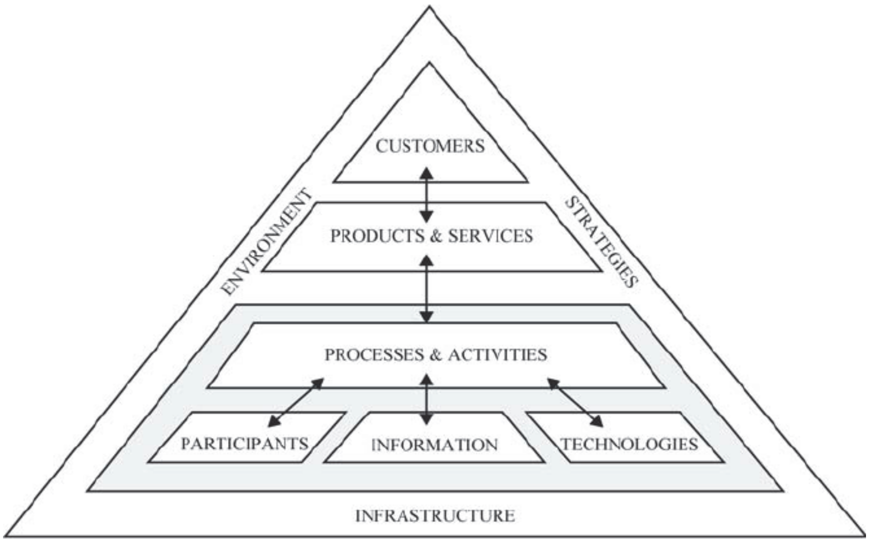


Figure 1. The work system Framework (Alter, 2008).

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).

2.2 Marturity Model Architectures

A maturity model identifies deficiencies in process structure and management, and unsatisfactory performance causes (Mayer & Fagundes, 2009). Based on the assumption of predictable patterns of organizational evolution and change, maturity models typically represent theories about how an organization’s capabilities evolve in a stage-by-stage manner along an anticipated, desired, or logical path. They give guidance through an evolutionary process by incorporating formality into the promising improvement activities (Mettler & Tobias, 2010).

Maturity models typically include a sequence of levels (or stages) that form an anticipated, desired, and logical path from an initial state to maturity (Röglinger, Pöppelbuß & Becker, 2012). An organization’s current maturity level represents its capabilities in regard to specific class of objects and application domain (Rosemann & de Bruin, 2005). Maturity models are used to assess as-is situations, to guide improvement initiatives, and to control progress (Iversen, Nielsen & Norbjerg, 1999). After defining the maturity level of an activity or process, the users have to define an improvement plan. The latter is the actions that must be achieved to reach a desired level maturity of the assessed activity.

There are three types of maturity model architectures (Steenbergen, Berg & Brinkkemper, 2007). The first two architectures are qualified as "Fixed Level Architecture". These are "staged" and "continuous" architectures. The staged architecture is characterized by several maturity levels (ML). Every level groups a set of maturity domains. A level is reached if all requirements of its domains are verified.

Table 1 illustrates the staged architecture which has n levels. Domain k having the level n means that all requirements of this domain for this level are verified. The organization can have different levels for different domains.

Table 1. Fixed Level (n) staged Architecture

	Level 1	Level 2	…	Level n
Domain 1	X			
Domain 2	X			
Domain 3		X		
…				
Domain k				X

The continuous architecture measures the domain's capacity. It defines a scale of skill levels for the latter. A domain reaches a level of aptitude if it satisfies all the corresponding requirements.

Table 2. Fixed Level (j) continuous Architecture

	Level 1	Level 2	…	Level j
Domain 1	X	X	X	X
Domain 2	X	X		X
Domain 3	X	X	X	
…	X	X	X	
Domain k	X	X	X	X

Table 2 illustrates the continuous architecture. An organization having the level j means that all corresponding domains verify the requirement of this level. In the same example, the activity has level 2.

The most recognized model in this architecture is Capability Maturity Model Integration (CMMI). The later addresses three areas of interest: Product and service development, Service establishment and management, and finally Product and service acquisition. It has level 5 for the both staged and continuous architectures. The CMMI-Like models are the models which use the CMMI architecture but for other disciplines. They are widely used but present certain limits. The most important limit, in the present research context, is the strong focus on formalization of improvement activities accompanied by extensive bureaucracy (Herbsleb & Goldenson, 1996), in absence of formal method which can help in fast, not expensive and reliable decision-making.

The third type is the test process improvement model proposed by (Koomen & Pol, 1999). This is the "Focus Area model" (FA). It is based on the idea that each area of maturity has its own evolution. It is interesting for assessing activity with interdependencies between their various domains. For this reason, the FA is the most adequate model for risk management process.

Table 3. Focus Area architecture

	Level 1	Level 2	…	Level m	…
Domain 1	X	X	X	X	
Domain 2		X			
Domain 3		X		X	X
…	X	X	X		
Domain k		X	X		X

Table 3 illustrates this architecture. The organization has level 2. But each domain has its own level. Domain 1 has level m. domain 2 has level 2. Etc. The FA model is detailed in section 2.3.

2.3 Focus Area Maturity Model

"Focus Area (FA)" (Steenbergen, Bos, Brinkkemper, Weerd, & Bekkers, 2010) is a maturity model design approach developed using the DSR (Design Science Research) process (Peffers, Tuunanen, Rothenberger & Chatterjee, 2008). FA Maturity models aim to support the continuous and progressive improvement of software testing (Koomen & Baarda, 2006).

A Focus Area is a well-defined coherent subset of a Functional Domain (Steenbergen, Bos, Brinkkemper, Weerd, & Bekkers, 2010). The total set of focus areas is a partition of the functional domain, i.e. different focus areas are disjointed and the union of all these focus areas is the complete functional domain (Steenbergen, Bos, Brinkkemper, Weerd, & Bekkers, 2010). In this category of models each focus area has its own number of specific maturity levels. The overall maturity of an organization is expressed as a combination of the maturity levels of these focus areas. The approach proposed by (Steenbergen, Bos, Brinkkemper, Weerd, & Bekkers, 2010) consists of four steps: (1) Scoping: identify and scope domain, (2) design model: determine focus area, capabilities, dependencies and position capabilities in matrix, (3) Instrument development: develop assessment instrument and define improvement actions, (4) implementation and exploitation: implement maturity model, improve matrix iteratively and communicate results.

The proposed approach illustrated in Figure 2 is modeled using the notation presented by (Weerd & Brinkkemper, 2008), which is based on standard UML conventions, with some minor adjustments.

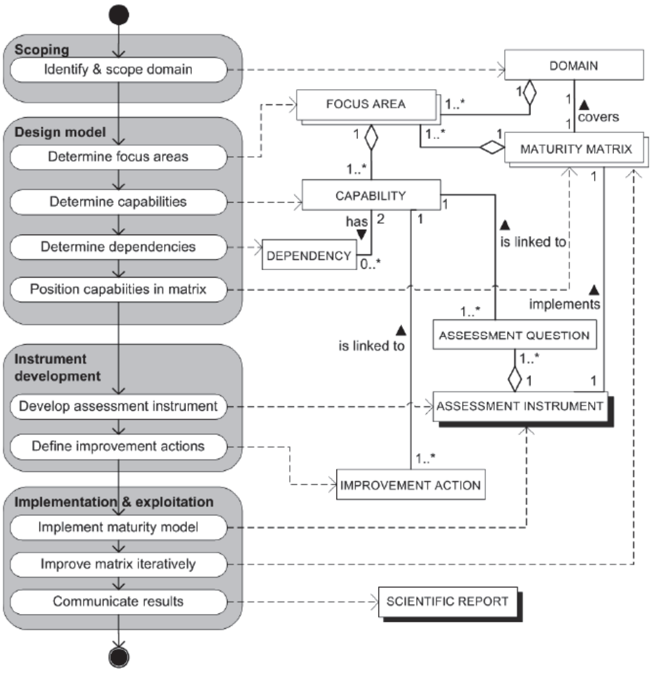
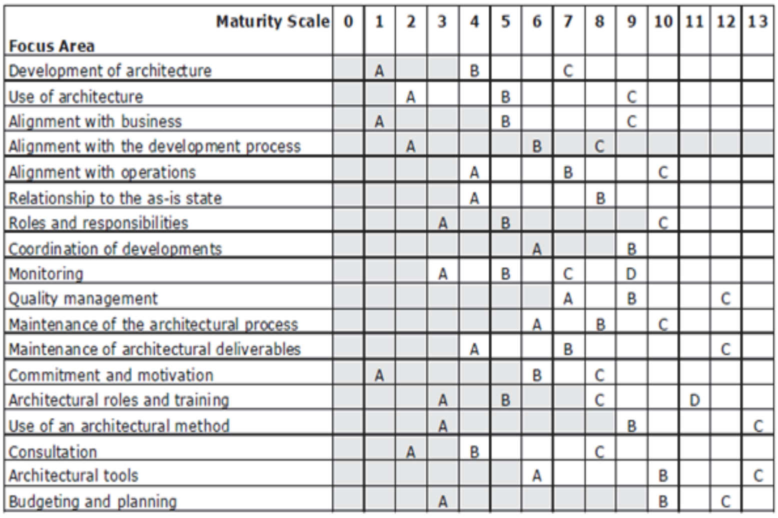


Figure 2. The development method for focus area maturity models (Steenbergen, Bos, Brinkkemper, Weerd, & Bekkers, 2010)

The maturity matrix is the key deliverable of the design phase. It includes FA capabilities (or Control Objectives (CO): A, B, C, etc.) which give a score for each activity domain or Focus Area. Those capabilities are based on their order and dependencies. It provides the level of maturity once the instrument designed and also defines improvement paths. Figure 3 shows an example of this matrix.



Maturity Scale Focus Area	0	1	2	3	4	5	6	7	8	9	10	11	12	13
Development of architecture		A			B			C						
Use of architecture			A			B				C				
Alignment with business		A				B				C				
Alignment with the development process			A				B		C					
Alignment with operations					A			B			C			
Relationship to the as-is state					A				B					
Roles and responsibilities				A		B					C			
Coordination of developments							A			B				
Monitoring				A		B		C		D				
Quality management								A		B			C	
Maintenance of the architectural process							A		B		C			
Maintenance of architectural deliverables					A			B					C	
Commitment and motivation		A					B		C					
Architectural roles and training				A		B			C			D		
Use of an architectural method				A						B				C
Consultation			A		B				C					
Architectural tools							A				B			C
Budgeting and planning				A							B		C	

Figure 3. Example of FA model maturity matrix

An organization reaches overall maturity level 'l' (0 <= l <= max levels defined in matrices) if:

- All capacities located in the column corresponding to the level 'l' are verified,
- All capacities located in the left of the column corresponding to the level 'l' are verified,
- There is at least one capacity on the right of the column corresponding to the level 'l' that is unverified.

Figure 3 gives an example of an FA maturity matrix. This later contains 18 domains and 13 levels. The first “development of architecture (DA)” has three control objectives: DA.A, DA.B and DA.C. the second domain ”use of architecture (UA)” has also three control objectives : UA.A, UA.B and UA.C. Table 4 illustrates the interdependencies between the control objectives of the two domains.

2.4 Information System Maturity Models

The CMM (Capability Maturity Model) is a guide for improving software development and maintenance practices. "It is composed of key practices that express the best way to work to produce quality software, with increased productivity and within budget and deadlines" (Basque, 2011). It's not dedicated to information system risk management, but its architecture is used in some other maturity models which deal this activity.

Capability Maturity Model Integration (CMMI) is an extension of the CMM. Its birth comes to answer the fear of confusion following the appearance of several models whose objectives differ from the initial objective of the CMM (examples: SE-CMM (for System Engineering), SA-CMM (for Software Acquisition), IPD -CMM (for Integrated Product Development) and even People-CMM, for human resources management).

This model is cited in this literature study as it is considered one of the most dominant foundations in previous SI research in terms of maturity models (Poeppelbuss, Niehaves, Simons, & Becker, 2011).

Figure 4 illustrates Unified Modeling Language (UML) modeling of the CMMI structural core (Deguil, 2008)

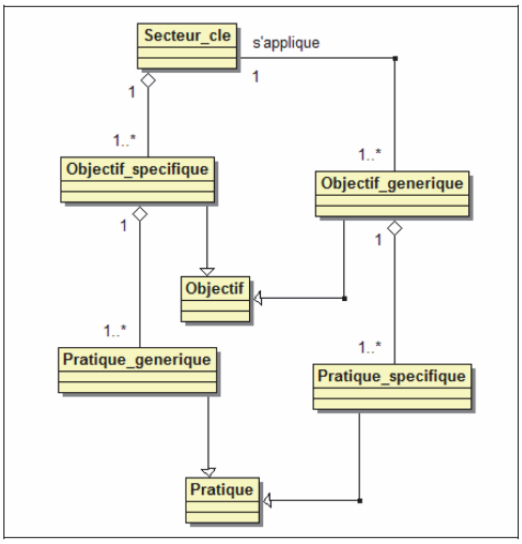


Figure 4. CMMI UML modelization (Deguil, 2008)

The said core makes interact the following components: - Good Practices: This concept does not only concern the CMMI but it represents a basic concept. According to the OMG "a good practice is a proven way or a strategy to accomplish a task in order to achieve a goal that would have a positive impact on the work products or the quality of the processes involved. ". In the context of a maturity or capacity model, the deployment of good practices is the tool for measuring capacity, and therefore maturity. This verification is done through the collection and analysis of evidence of deployment (Deguil, 2008). The CMMI distinguishes two types of practices: specific and generic. - Specific practices: specific practices aim to satisfy the purpose of a particular process area. Two different process domains can not contain the same specific practices. - Generic practices: Generic practices are transversal to all process areas. They make it possible to ensure that the associated process is efficient and reproducible (Deguil, 2008). - Objectives: a set of practices can contribute to the achievement of a given objective. The latter is also divided into generic and specific objectives. - Key sectors: A key sector (PA - Process Area1) is, in turn, a particular area on which an organization must focus in order to improve its software process (Deguil, 2008). In CMMI, the key sectors are groups of objectives (and therefore, indirectly, practices) (Deguil, 2008).

The CMMI can be used in two types of representation: continuous and staged. The tiered representation expresses the evolution of practices according to a more global or organizational view (Basque, 2011). This evolution is made according to five levels of maturity: (1) level 1: "initial", (2) level 2: "disciplined", (3) level 3: "adjusted", (4) level 4: "managed quantitatively" , and (5) level 5: "in optimization". As for the continuous representation, she is interested in the evolution of the processes rather than that of the whole organization. The concept of maturity of the organization is replaced by the capacity of a process. Indeed, continuous representation expresses the capacity or ability of each process taken separately within the organization (Basque, 2011). This capacity is evaluated on a scale of 0 to 5. Continuous representation allows greater flexibility for the organization as it offers a choice in the order of implementation of key sectors (Reifer, 2000).

The MMGRSeg model measures the maturity level of the information security related to risk management process (Mayer & Fagundes, 2009). It is aligned with ISO / IEC 27005. It has three stages of maturity (Mayer & Fagundes, 2009): (1) immaturity: the organization processes are improvised or not respected, (2) maturity: organizational processes are already defined, standardized and controlled and (3) excellence: the organization is able to optimize its processes as they are all engaged in continuous improvement activities. A controlled advancement of technologies and processes takes place.

The domains of the MMGRSeg model are the six activities of the ISO / 27005 risk management processes: (1) context definition, (2) risk analysis / evaluation, (3) risk treatment, (4) risk acceptance, (5) communication and (6) analysis and monitoring.

These domains are evaluated according to five levels of maturity: (1) initial: the company has a basic knowledge of a given activity of the risk management process, but the process is not yet implemented, (2) known: organization has good knowledge of a given risk management process activity, but only certain individuals in the field of information security have this good knowledge. These are the people who perform the activity assigned in an intuitive way, ie no formal approach is developed for the relevant activity of the risk management process, (3) standardized: with Using a methodology, the company adopts a standard to perform a given activity of the risk management process. This methodology should be aligned with the guidelines of ISO / IEC 27005, (4) managed: the activities of the risk management process are audited. This audit is conducted through a thorough and systematic review to verify whether the activities are in line with the planned and / or previously implemented parameters, if they have been implemented effectively, and if they are sufficient to achieve the objectives. There is a wide range of knowledge among the entire team regarding the activities of the information security risk management process (Mayer & Fagundes, 2009), (5) optimized: the activity has reached a level of excellence because it manages to eliminate deficits, failures and re-machining

The model presented proposes 43 control objectives distributed over its six domains. A control chart defines for each level of maturity the control objectives to be verified.

The MMGRSeg model also proposes a RACI matrix defining the responsibilities of the different actors in relation to the achievement of control objectives.

The evaluation system is based on a questionnaire of 35 questions, the first two of which are designed to evaluate level 1 of the six domains. The remaining questions are broken down by level and field of maturity. The questionnaire uses the Likert scale. The literature studied does not provide the way of scoring the questionnaire.

RISK IT is a framework proposed by the Information Systems Audit and Control Association (ISACA) for IT risk management. It is composed of three areas (ISACA, 2010): (1) risk governance, (2) risk assessment, and (3) risk response. It proposes for each of these domains a model of maturity.

These three models focus on six areas (ISACA, 2010): awareness and communication, (2) responsibilities and accountability, (3) definition of objectives and associated measures, (4) policies, standards and procedures, (5) skills and expertise, and (6) tools and automation. Risk IT defines six levels of maturity (from 0 to 6) (ISACA, 2010): (0) process not applied, (1) process ad hoc and disorganized, (2) process following a regular pattern, (3) processes documented and communicated, (4) monitored and measured process, and (5) best practices followed and automated. Risk IT is integrated in the new Cobit 5 version of COBIT.

(Elmaallam & Krioule, 2012-b)) proposed a IS risk management maturity model with five levels:

- Level 1, initial: The work is based on individual initiatives. No methodology or procedure (based on the bestpractices) formalized and normalized. Everyone manages the risks in his way. The result is unpredictable.

- Level 2, defined: There is an effort from stakeholders to use best practices. However, there are no standard methods or common criteria for evaluating results.

- Level 3, Normalized: For each activity of the risk management process there are formalized and normalized techniques.

- Level 4, Managed: A knowledge base is built, and it includes the return on experience. We begin to measure the effectiveness and the relevance of risk management activities.

- Level 5, Optimized: Risk management activities are part of a continuous improvement process based on the results and measurements of the level 4.

For each IS of the company:

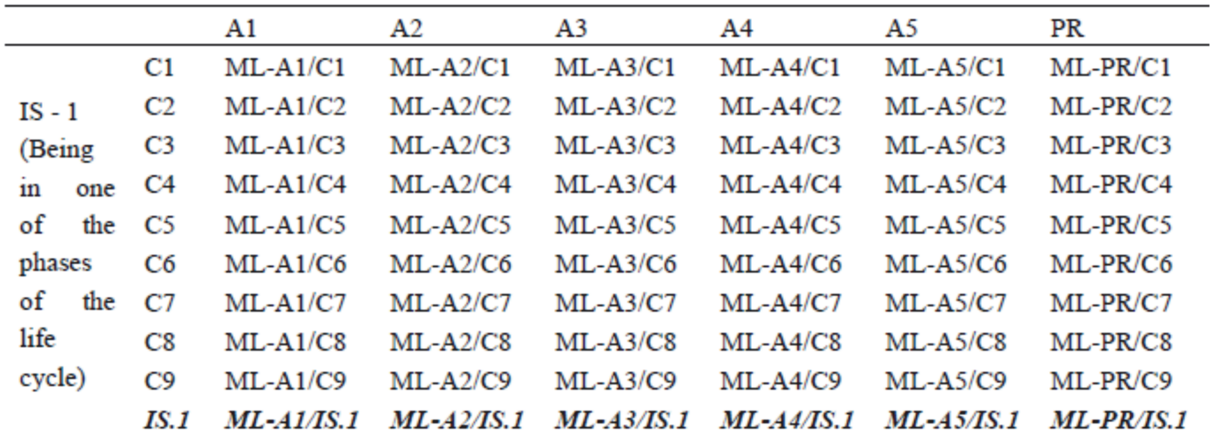
- Determine its nine constituents

- Assess the level of maturity for each activity and constituent

- Assess the level of maturity of each activity by a formula that consolidates the all constituents with its weights for the IS

- Assess the level of maturity of the whole process by a formula that consolidates the all activities

This model can be represented under the matrix shape mentioned in the Figure 5 (Elmaallam & Kriouile, 2012-b).



		A1	A2	A3	A4	A5	PR
IS - 1 (Being in one of the phases of the life cycle)	C1	ML-A1/C1	ML-A2/C1	ML-A3/C1	ML-A4/C1	ML-A5/C1	ML-PR/C1
	C2	ML-A1/C2	ML-A2/C2	ML-A3/C2	ML-A4/C2	ML-A5/C2	ML-PR/C2
	C3	ML-A1/C3	ML-A2/C3	ML-A3/C3	ML-A4/C3	ML-A5/C3	ML-PR/C3
	C4	ML-A1/C4	ML-A2/C4	ML-A3/C4	ML-A4/C4	ML-A5/C4	ML-PR/C4
	C5	ML-A1/C5	ML-A2/C5	ML-A3/C5	ML-A4/C5	ML-A5/C5	ML-PR/C5
	C6	ML-A1/C6	ML-A2/C6	ML-A3/C6	ML-A4/C6	ML-A5/C6	ML-PR/C6
	C7	ML-A1/C7	ML-A2/C7	ML-A3/C7	ML-A4/C7	ML-A5/C7	ML-PR/C7
	C8	ML-A1/C8	ML-A2/C8	ML-A3/C8	ML-A4/C8	ML-A5/C8	ML-PR/C8
	C9	ML-A1/C9	ML-A2/C9	ML-A3/C9	ML-A4/C9	ML-A5/C9	ML-PR/C9
	IS.1	***ML-A1/IS.1***	***ML-A2/IS.1***	***ML-A3/IS.1***	***ML-A4/IS.1***	***ML-A5/IS.1***	***ML-PR/IS.1***

Figure 5. Illustration of IS risk management maturity model (Elmaallam & Kriouile, 2012-b)

2.5 Comparative Analysis

The comparative analysis of maturity models aims to evaluate them based on a set of well-defined criteria. These criteria are:

- C1: Genericity: the proposed solution must be generic from the point of view of the IS risk management process and concept,
- C2: Independence of the context of application: The solution must be applicable in all the contexts and sectors of activity,
- C3: Adaptability: The solution must make it possible to take into account the specificities of the context where the model is applied,
- C4: Transparency: The solution must ensure the documentation and the traceability of the measures of maturity,
- C5: Improvement plan: does the model assist its users in defining an improvement plan?
- C6: Theoretical basis: is the model based on the theoretical aspect of the domain studied for measuring maturity?
- C7: Relevance and adequacy to requirements (IS RM).

Table 4 presents the result of the evaluation of the maturity models presented in section 2.3 according to the criteria mentioned above.

Table 4. Maturity models evaluation

Modèle	C1	C2	C3	C4	C5	C6	C7	% fitting criteria
CMMI	-	+	-	+	-	-	-	29%
MMGRSeg	+	+	-	-	-	-	-	29%
Risk IT	-	+	-	+	-	-	-	29%
(Elmaallam & Kriouile, 2012-b)	+	+	+	+	-	+	-	71%

The evaluation results show that the correspondence of the existing risk management and IS risk management maturity models to the evaluation criterion is too weak. Only C2 and C4 criteria are verified by most models. The model proposed by (Elmaallam & Kriouile, 2012-b) verifies 71% of criteria. It needs to be improved specially in the two criterias: C5 and C7 since it does not assist its users in defining an improvement plan and does not take in consideration the interdependence between risk management activities.

In this paper, we focus on C7criteria and propose a maturity model for assessing the information system risk management.

3. Information System Risk Management Maturity Model

The Information Systems Risk Management Maturity Model aims to evaluate information system (IS) risk management. An IS is defined as a special case of work system (Alter & Sherer, 2004) in which A work system is a system in which human participantsand/or machines perform work (processes and activities) using information, technology, and other re-sources to produce specific products and/or services forspecific internal or external customers. As for the risk management, the proposed model adopts the ISO 31000 Framework (ISO, 2009) with the generic management cycle proposed by Sienou (Sienou, 2009). This cycle resumes the stages of the process proposed by ISO 31000 with a restructuring of its phases. Indeed: (1) communication is considered as an activity inherent to every phase of the process (Sienou, 2009), (2) the cycle of management preserves its iterative character, but no longer requires synchronization of all stages with a monitoring phase (Sienou, 2009), and (3) Treatment may be the cause of a new iteration process (Sienou, 2009).

The development of the target model should provide answers to the problem of assessing IS risk management from two perspectives. The first perspective is academic. The model must address a problem not sufficiently addressed in IS research: the assessment of IS risk management. The proposed solution must also be able to open new perspectives and opportunities in scientific research in this area. The second perspective relates to the practical side. The proposed model should be easy to implement and comply with the best practices of risk management.

This model aims to satisfy seven principal requirements: (1) Genericity, (2) Independence of application context, (3) adaptability, (4) transparency, (5): plan improvement, (6) Theoretical basis and (7) Need adequacy (IS RM topic). It's structured along two dimensions. The first dimension includes evaluated activities. It is a matter of risk management activities. The second dimension represents the aspects under which these activities are evaluated. It is a matter of evaluation axes and elements related to an IS defined as a WS.

The maturity assessment is made according to the "Focus Area" architecture. The choice is justified by the fact that this architecture provides a more sophisticated approach than the other two architectures in relation to the purpose and scope of the proposed model. Indeed, it defines small evolutionary steps thus making improvement easier, less risky, less costly and clearer. The choice is also justified by taking into account the control objectives interdependencies which is an important characteristic of the risk management business.

3.1 Domains and Domains Groups

The areas adopted for the proposed model are the risk management activities. It is deducted from Risk Management Framework proposed by ISO 31000. The domain groups are the three pillars of the ISO 31000 Framework. We have added the "Recording" section.

The areas of maturity are then listed in Table 5. For the domain group "Process", the maturity domains of selected areas are sub-activities of each of its activities. This is justified by the fact that this level reflects more the operational component of the process.

Table 5. Information system risk management maturity model domains

Domain group	**Domain**
RM principle	RM principle
Organizational framework of risk management	Mandate and commitment
	Design of framework
	Implement risk management
	Monitor and review framework
	Improve framework
Process	External context
	Internal context
	Process context
	RM criteria
	Risk identification
	Risk analysis
	Risk evaluation
	Selection of treatment options
	Development of the treatment plan

Domain group	Domain
	Implementation of the treatment plan
	Monitoring and review
Recording	Recording

3.2 Axes and Elements of Evaluation

The areas of assessment are the elements of the IS defined as WS (Alter & Sherer, 2004). These are: (1) infrastructure, (2) strategy, (3) environment, (4) technology (5) Information (6) participants, (7) process (8) products, and (9) customers.

The evaluation elements of each axis are identified through (1) the missions and requirements of WSF as defined in the literature (Alter & Sherer, 2004), (2) the application of the theory RBV (Resource Based-view) (Wade & Hulland, 2004) on IS defined as WS considering both dynamic resources such as skills, as static as the technical infrastructure, (3) the IS risk factors(Alter & Sherer, 2004), and (4) interviews with IS experts. Table 6 lists the evaluation elements for each component.

Table 6. Information system evaluation elements

Axis	Evaluation element	Axis	Evaluation element
Infrastructure	Technical infrastructure	Information	Security
	Human infrastructure		Reliability
	Informational infrastructure		Relevance
Strategy	Alignment	Process	Agility
	Contribution		Formalization
Environment	Organism		Updating
	Culture		Interaction
	Intra Enterprise regulations		Coherence
IT	competitive importance	Product	Compliance with requirements
	complexity		Quality
	Codifiability		Exploitation
	Potential of credibility		Needs
	Strategic profile	Customer	Satisfaction
Participants	Competence		Competence
	Cooperation		Cooperation
	stability		

3.3 Control Objectives

The objectives of control describe the way of progressive improvement of a maturity domain. To define them, we used: (1) description of Framework of risk management given by the standard ISO 31000, (2) study of the literature, and (3) focuses group and interview with risk management experts.

A control objective is identified via the following elements: (1) code, (2) name, (3) target (4) actions needed for its implementation, (5) prerequisite control objectives on which it depends, (6) estimated load, (7) estimated cost of implementation, and (8) implementation of impact.

For example, the control objectives defined for the RM principles domain are:

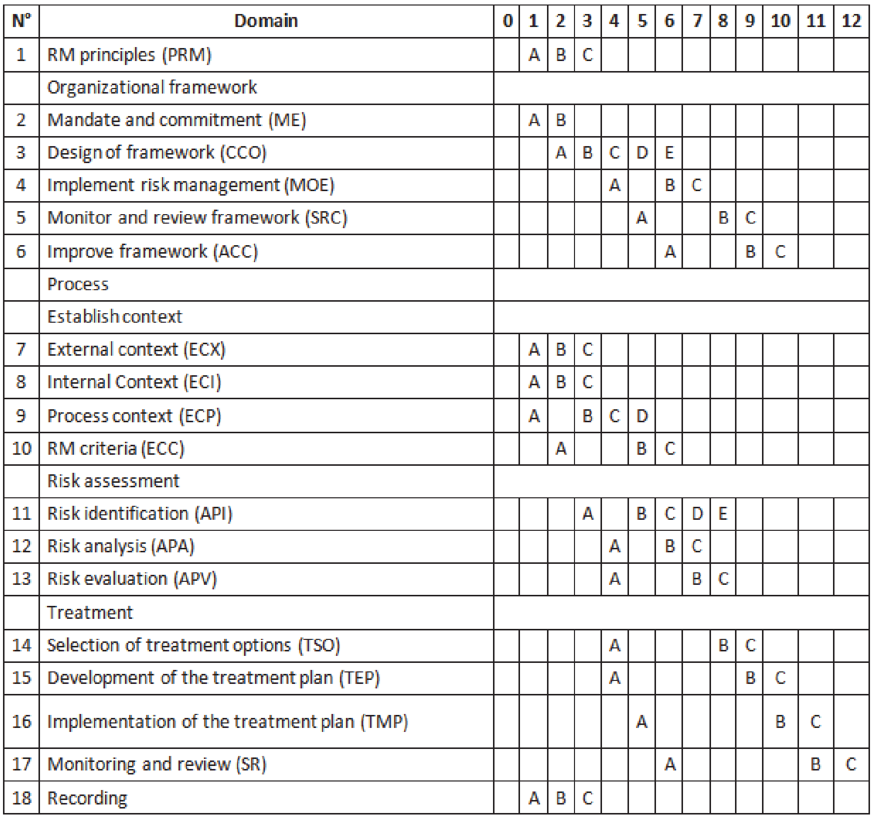
- A: Reminded principles
- B: Principles formalized and communicated
- C: Principles evaluated in terms of understanding and adherence

3.4 Maturity Matrix

The position of the control objectives (CO) in the maturity matrix is defined by calculating their ranks according to the rule (1).

The application of this rule allows obtaining the matrix of maturity illustrated in figure 6.

If the CO is independent of all others CO, then rank (CO) = 1. If the CO depends on a number of other CO: {CO1, CO2, .., COn}, then the rank is calculated as rank (CO) = Max (COi) +1, 1 <= i <= n. (1)



N°	Domain	0	1	2	3	4	5	6	7	8	9	10	11	12
1	RM principles (PRM)		A	B	C									
	Organizational framework													
2	Mandate and commitment (ME)		A	B										
3	Design of framework (CCO)			A	B	C	D	E						
4	Implement risk management (MOE)					A		B	C					
5	Monitor and review framework (SRC)						A			B	C			
6	Improve framework (ACC)							A			B	C		
	Process													
	Establish context													
7	External context (ECX)		A	B	C									
8	Internal Context (ECI)		A	B	C									
9	Process context (ECP)		A		B	C	D							
10	RM criteria (ECC)			A			B	C						
	Risk assessment													
11	Risk identification (API)				A		B	C	D	E				
12	Risk analysis (APA)					A		B	C					
13	Risk evaluation (APV)					A			B	C				
	Treatment													
14	Selection of treatment options (TSO)					A				B	C			
15	Development of the treatment plan (TEP)					A					B	C		
16	Implementation of the treatment plan (TMP)						A					B	C	
17	Monitoring and review (SR)							A					B	C
18	Recording		A	B	C									

Figure 6. Maturity matrix

3.5 Evaluation System

In order to build this system, we use an approach based on the principle of the method GQM (Goal-Question-Metric) (Basili, Caldiera & Rombach, 1994). This process involves the following steps:

- Determine the objectives of the evaluation system (Goal): The system of evaluation has for objective to estimate the domains of maturity through the evaluation of the realization of the corresponding control objectives. This allows fulfilling the matrix of maturity pre-established according to the verified OC and to define the level of maturity of the risk management of IS studied. There are 18 goals. They can be so formulated as: Gi: " estimate the domain of maturity Di ", 1 =< i =< 18,

- Formulate questions (Question) to identify aspects to be measured to assess the achievement of defined objectives. In light of defined objectives, questions can be formulated in the following way: Qi: "In what stage of development is the domain Di?" (1 <= i = <18),

- Define metrics (Metric) to evaluate these aspects: Metric responding to the question Qi Di for each domain are related control objectives,

- Define the elements to measure these metrics: these elements, called in the proposed model : control elements, are specifically defined for each control objective from its requirements.

Table 7 shows an example of the definition of the control elements: PRM.C: "Principles evaluated in terms of understanding and adherence" of domain "RM principles”.

Table 7. Example of control element

OC	OC goal	Aspect to be verified	Elements of control of the OC
Principles evaluated in terms of understanding and adherence.	Assess the understanding and application of risk management principles.	-Understanding of risk management principles -Application And adherence to risk management principles	-Does the organism measure the level of understanding of IS risk management principles (surveys, quizzes ...)? - Does the organism measures the degree of adherence to IS risk management principles (surveys, quizzes ...)?

A control objective is checked whether all control elements have a favorable response ie equal to "yes."

The evaluation is done through a self-assessment questionnaire. The latter is formed from the control elements previously defined. It is divided into three categories according to three categories of evaluation: (1) category 1: organism, (2) category 2: IS, and (3) category 3: IS with considering axes and elements evaluation.

This questionnaire according to its three categories is implemented in Excel.

For purposes of consolidation measures made by control elements, the answers are translated into quantitative values: "Yes" = 1 and "no" = 0.

The first category concerns the management of the IS risks at the level of the organism in a global way. it concerns in particular domains belonging to the groups of domains " RM principles" and " organizational framework". A control objective is considered achieved if all the answers to the relevant questions (control elements) are "yes".

The second category concerns studied IS. However, the questions are not declined in axes and elements of evaluation. An objective of control is considered reached if all the answers to the corresponding questions (elements of control) are in "yes". The activity "recording" and "the treatment" are examples.

The third category requires checking elements of control of a domain at the level of every evaluation element of the studied IS. This questionnaire allows to consider the specificities of every organism through a configuration variable called "Applicable" indicating the applicability or not of an element of evaluation and if it presents an eliminatory characteristic. The Measure of a control element (EC) relative to an evaluation axis (IS elements) is the rounded value of the arithmetic mean of the measurements of its evaluation elements taking into account the settings of variable values (2).

$$\text{Measure\_EC (Axe\_Eval)} = \text{Round [mean (Mesure\_EC (Elt\_Eval i)} \times \text{Valeur\_Applicable (Elt\_Eval i))]}; 1 <= i <= \text{number of assessment items in Axe\_Eval} \quad (2)$$

The questionnaire also takes into consideration the IS lifecycle. Indeed, the measure of a control element is the rounding of the weighted average of its measurements by axis evaluation (3). The weight (Axe_Eval) of this weighting is the importance of each axis evaluation in the phase of the life cycle of the information system at the time of the evaluation. In the absence of studies dedicated to the calculation of this weight, we propose to hold focus groups to define for each type of SI as the context of the business.

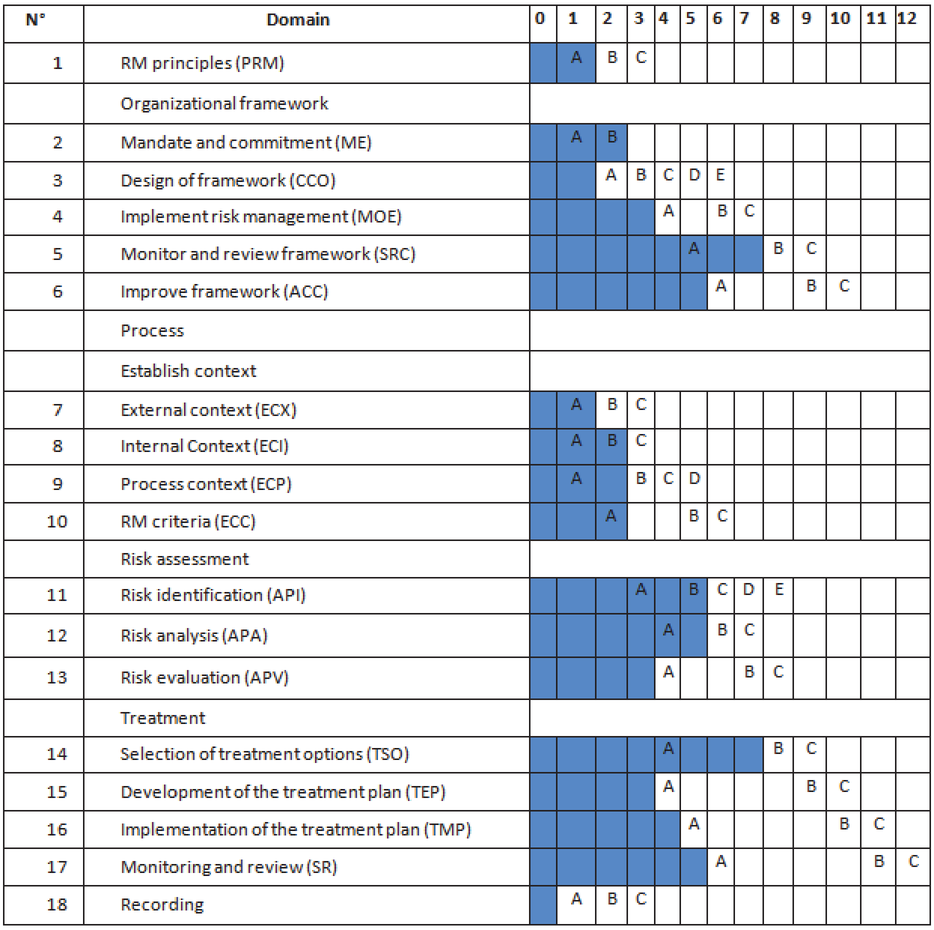
$$\text{Measure (EC)} = \text{Round [Sum (weight (Axe\_Eval j)} \times \text{Mesure\_EC (Axe\_Eval j))]}; 1 <= j <= 9 \text{ (number of evaluation axes = 9)} \quad (3)$$

The measure of a control objective is "yes" if all the corresponding questions are "yes" (value 1) and "no" (value 0) otherwise (4).

$$\text{Measure (OC)} = \text{product (Measure (EC i))}; 1 <= i <= \text{number of EC in OC} \quad (4)$$

Once the control objectives evaluated, the matrix is populated. The lines of each domain are marked with a different color until the corresponding cell to the maximum value of the ranks of control verified objectives. The maturity level of IS risk management for each domain group is the one corresponding to the right column which all the cells harboring the required control objectives are colored. Figure 3 gives an example of the filled matrix.

The company may have a global view of the maturity of its IS risk management through the consolidation of its various IS measures. Indeed, for each maturity domain, the overall rank is the rounding of the weighted average of the ranks in each IS. Quantitative values for each control objective are the corresponding ranks at the maturity scale. For example, in the matrix shown in Figure 3, the value corresponding to the control objective "D" verified by the CCO field is "5". The consolidation weight is the weight of the IS reflecting its importance in the organism strategy.



N°	Domain	0	1	2	3	4	5	6	7	8	9	10	11	12
1	RM principles (PRM)	■	A	B	C									
	Organizational framework													
2	Mandate and commitment (ME)	■	A	B										
3	Design of framework (CCO)	■	■	A	B	C	D	E						
4	Implement risk management (MOE)	■	■	■	■	A		B	C					
5	Monitor and review framework (SRC)	■	■	■	■	■	A	■	■	B	C			
6	Improve framework (ACC)	■	■	■	■	■	■	A			B	C		
	Process													
	Establish context													
7	External context (ECX)	■	A	B	C									
8	Internal Context (ECI)	■	A	B	C									
9	Process context (ECP)	■	A	■	B	C	D							
10	RM criteria (ECC)	■	■	A			B	C						
	Risk assessment													
11	Risk identification (API)	■	■	■	A	■	B	C	D	E				
12	Risk analysis (APA)	■	■	■	■	A	■	B	C					
13	Risk evaluation (APV)	■	■	■	■	A			B	C				
	Treatment													
14	Selection of treatment options (TSO)	■	■	■	■	A	■	■	■	B	C			
15	Development of the treatment plan (TEP)	■	■	■	■	A					B	C		
16	Implementation of the treatment plan (TMP)	■	■	■	■	■	A					B	C	
17	Monitoring and review (SR)	■	■	■	■	■	■	A					B	C
18	Recording	■	A	B	C									

Figure 7. Example of maturity matrix

4. Conclusion

In this paper, we propose a maturity model for assessing information system risk management. Indeed, the comparative analysis based on the literature study shows that none of the existing maturity models deals with the dependencies between the information system risk management elements. The main contribution of the proposed model is then to consider this constraint by using the Focus Area architecture.

For future work, we intend to develop a method helping the proposed maturity model users in defining the improvement plan once the assessment is done.

References

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.

Basili, R. V., Caldiera, G., & Rombach, H. D. (1994). Goal/Question /Metric Paradigm. *Encyclopedia of Software Engineering, 1,* 528-532.

Basque, R. (2011). CMMI 1.3 - Guide complet de CMMI-DEV et traduction de toutes les pratiques CMMI-ACQ et CMMI-SVC. Dunod.

De Courcy R. (1992). Les systèmes d'information en réadaptation. *Québec, Réseau international CIDIH et facteurs environnementaux, 1*(5), 7-10.

Deguil, R. (2008). Mapping entre un référentiel d'exigences et un modèle de maturité :application à l'industrie pharamceutique. Toulouse, France: Institut National Polytechnique de Toulouse.

El maallam, M & Kriouile, A, (2012). A Model of Maturity for IS Risk Management Case Study. *Computer and Information Science (CIS), 5*(3), 97-109. https://doi.org/10.5539/cis.v5n3p97.

Elmaallam, M, & Kriouile, A. (2013). “Toward a Maturity Model Development Process for Information Systems (MMDePSI).” *IJCS International Journal of Computer Science Issues, 10*(3), 118-125.

Elmaallam, M., & Kriouile, A. (2012). “Model ISR3M for assessing maturity of IS risk management process Case study”. CIST' 12, Colloquium on Information Science and Technology, Fez, Morrocco. 2012.

Herbsleb, J. D., & Goldenson, D. R. (1996). A systematic survey of CMM experience and results. Proceedings of the 18th international conference on Software engineering (pp.323-330). Washington, DC, USA: IEEE Computer Society.

ISACA. (2010). RISK IT Framework.

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

Iversen, J. H., Nielsen, P. A., & Norbjerg, J. (1999). Situated Assessment of Problems in Software Development. *DATA BASE, 30*(2), 66-81.

Koomen, T., & Baarda, R. (2006). TMap Test Topics. UTN Publishers.

Koomen, T., & Pol, M. (1999, Junr). Test Process Improvement, a practical step-by-step guide to structured testing. Addison-Wesley Professional.

Mayer, J., & Fagundes, L. L. (2009). A Model to Assess the MaturityLevel of the Risk Management Process in Information Security. 4rd IFIP/IEEE International Workshop on BDIM. New York.

Mettler, T. (2010). Thinking in Terms of Design Decisions When Developing Maturity Models. *International Journal of Strategic Decision Sciences (IJSDS), 1*(4), 76-87.

Peffers, K., Tuunanen, T., Rothenberger, M. A., & Chatterjee, S. (2008). A Design Science Research Methodology for Information Systems Research. *Journal of Management Information Systems, 24*(3), 45-77.

Poeppelbuss, J., Niehaves, B., Simons, A., & Becker, J. (2011). Maturity Models in Information Systems Research: Literature Search and Analysis. *Communications of the Association for Information Systems (AIS), 29*(27), 505-532.

Reifer, D. J. (2000). The CMMi it's formidable. *Journal of Systems and Software, 50*(2), 97-98.

Röglinger, M., & Pöppelbuß, J., & and Becker, J. (2012). Maturity Models in Business Process Management. *Business Process Management Journal, 18*(2), pp. 328-346.

Rosemann, M., & de Bruin, T. (2005). “Towards a Business Process Management Maturity Model,”. European Conference on Information Systems (ECIS), Regensburg, Germany. 2005.

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.

Steenbergen, M. v., Berg, M. v., & Brinkkemper, S. (2007). A Balanced Approach to Developing the Enterprise Architecture Practice. *Enterprise Information Systems, 12,* 240-253.

Steenbergen, M.V, & Bos, R., & Brinkkemper, S., & Weerd, I., & Bekkers, W. (2010). “The Design of Focus Area Maturity Models”. Proceedings of the 5th International Conference on Design Science Research in Information Systems and Technology St. Gallen, Switzerland, pp. 317-332, 2010.

Wade, M., & Hulland, J. (2004). Review: The resource-based view and information systems research: Review, extension, and suggestions for future research. *MIS Quarterly, 28*(1), 107-142.

Weerd, I. v., & Brinkkemper, S. (2008). Meta-modeling for Situational Analysis and Design Methods. Handbook of Research on Modern Systems Analysis and Design Technologies and Applications, 38-58.

Copyrights