SOCIETY FOR SCIENCE AND EDUCATION UNITED KINGDOM
TMLAI TRANSACTIONS ON MACHINE LEARNING AND ARTIFICIAL INTELLIGENCE
VOLUME 2, ISSUE 6
ISSN: 2054 - 7390

Development of the ISR3M Model for IS Risk Management Evaluation using the Focus Area Structure according to the MMDPIS Generic Process

[1]Mina El maallam and [2]Abdelaziz Kriouile
IMS Team, SIME Lab., ENSIAS, University Mohammed V-Souissi, Rabat, Morocco;
[1]elmaallam@gmail.com; [2]kriouile@ensias.ma

ABSTRACT

Risk management (RM) is one of the main IS governance pillars. However, to remain a center of profit and cost optimization for the company, this activity must be evaluated, monitored and improved continuously. Hence the interest to develop an IS risk management maturity model. This paper aims to address this need by providing the ISR3M (Information System Risk Management Maturity Model) model. After a summary of literature review, it presents the design approach, then describes the model and evaluates it.

Keywords: Information system, risk management, Maturity, Maturity model, Focus Area structure.

1 Introduction

Information System (IS) 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 also has an important role in making good decisions about entering new opportunities. In addition, it promises an optimal allocation of resources [1]. However, it presents a set of challenges for both professionals and researchers.

Indeed, a primary mission of Risk Managers is to help companies maximize profit through minimizing the cost of risk [2]. The latter being a combination of the cost of risk management and loss due to their eventual realization [3].

But "we can control only what we can measure" and we can measure only what we know. The first challenge is then raised to know the status of the IS risk management. The second challenge is to improve this activity to ensure efficiency and continuity of its implementation.

The present article aims to answer these challenges by proposing the ISR3M (Information System Risk Management Maturity Model) maturity model for IS risk management. This model has for objective to evaluate the maturity of risk management and ensure its continuous improvement through the implementation of small changes, frequent, incremental, quickly obtained [4] and guided by kaizen philosophy of "better than yesterday, less than tomorrow".

The second section presents a summary of literature review. It evokes the problems covered by section as well as a comparative study of existing solutions. The third section describes the approach adopted

DOI: 10.14738/tmlai.26.793
Publication Date: 05th January, 2015
URL: http://dx.doi.org/10.14738/tmlai.26.793

for the ISR3M design. This is the MMDPIS process [5]. The proposed model is presented in fourth and fifth sections and evaluated in sixth section. The paper is concluded in section seven.

2 Literature review

The interest of IS maturity models increases both for the researchers and for the professionals. However, their development and adoption still face several problems [6] especially for IS risk management discipline. There are two natures of problems.

The first is related to the definition of the studied field. Indeed, one of the problems hindering the IS risk management is the ambiguity that prevails. In IS, the risks interpretations differ from community to community [1]. In addition, IS risk management does not cover all aspects of the IS and is, in most cases, related to IT aspects.

The second problem is related to the model design. The latter presents numerous points of improvement such us:

- Lack of satisfactory answers to the implementation of improvement actions: the objective of the maturity assessment models is to identify gaps that could be filled by improvement actions [7]. However, most of these models do not describe how to effectively carry out these actions to deal with identified gaps ([8], [9], [10]).
- Falsified Certainty given to the decision-makers: another one critical, often shown, is that maturity models can give in the decision-makers a "falsified certainty" regarding the diagnosis and the evaluation of maturity. This report can be due to the carelessness of certain important aspects of the studied domain. It is also due to the very limited understanding of the reality ([8], [9]). For example, ([11]), [12], [13], [14]) qualify the models of maturity as "recipe stage by stage" which simplify excessively the reality.
- Poor theoretical basis: The third point considered by [15] as the most important criticisms of the existing maturity models are their poor theoretical basis. Indeed, most models are based on "best practices" or "success factors" from projects that have favorable results to a company or an industry [8]. Thus, to be consistent with the maturity model would not necessarily guarantee that the company would be successful [8]. There is no agreement on a "right way" to ensure a positive result [16].
- Lack in tests of model validity: According to [12], the ambiguity noted in results of maturity models lies in the insufficient emphasis on models testing in terms of validity, reliability and genericity. [8] confirms this and thinks the maturity models are a foundation that lack of experimentation.
- Not adequacy to the specific needs: other criticisms refer to the multitude of almost identical maturity models and to the not thoughtful adoption of the CMM main plan ([17], [18], [19]). The carelessness of the specific needs can hinder the achievement of the objectives of the maturity model. In the same line, [10] think that the maturity models must be customizable, because the internal and external characteristics can limit the applicability of a maturity model in its normalized version [19]. On the other hand, the design of the model in question must consider the context in which it will be deployed. The context is "all information that can be used to characterize the situation of an entity" [20].

- The high level of formalism: [21] think that too much emphasis on the formalization of improvement activities accompanied by extensive bureaucracy can block people innovation. [13] postulate that maturity models should not focus on one level sequence to an "end state" predefined, but on factors driving the evolution and change. The exaggerated formalism can also urge to remain motionless on a single path of improvement. In such cases, the models of maturity tend to neglect the potential existence of several paths so advantageous [22] and being able to better answer the possible evolutions in studied IS.

The review of the literature also concerned a comparative study of the maturity models in risk management and IS risk management. In the light of both natures of problems expressed previously, the proposed criteria of comparison are:

- C1: Genericity: the proposed solution should be generic viewpoint processes and IS risk management concepts.
- C2: independence of the context of application: the solution must be applicable in all the contexts and the business sectors.
- C3: Adaptability: The solution must take into account the specificities of the studied area.
- C4: transparency: the solution has to insure the documentation and the traceability of the maturity measures.
- C5: plan improvement: does the model assist its users in the definition of an improvement plan?
- C6: theoretical Basis: does the model based on the theoretical aspect of the domain studied for the measure of the maturity?
- C7: adequacy to needs (IS RM): is the model adapted to the IS risk management?

Table 1 shows the result of this study.

Table 1: Comparative study of RM maturity models.

Model	C1	C2	C3	C4	C5	C6	C7
RMM [23]	-	+	-	-	-	-	-
Project RMM [24]	-	+	-	+	-	-	-
COPS [25]	-	+	-	+	-	-	-
J-RMMM [26]	-	-	-	+	-	-	-
ERMM-Level Assessment Tool [27]	+	+	-	+	-	-	-
CMMI [28]	-	+	-	+	-	-	-
MMGRSeg [29]	+	+	-	-	-	-	-
Modèle de maturité de Risk IT [30]	-	+	-	+	-	-	-

The natures of the problems being so defined in a rather clear and precise way, the proposed answer is the design of a new model of maturity of the IS risk management: ISR3M. This model is developed using the MMDPIS process [5] described in section 3.

3 MMDPIS Process Description

The MMDPIS process is structured in three blocks: (1) design, (2) implementation, and (3) continuous improvement (Figure 1).

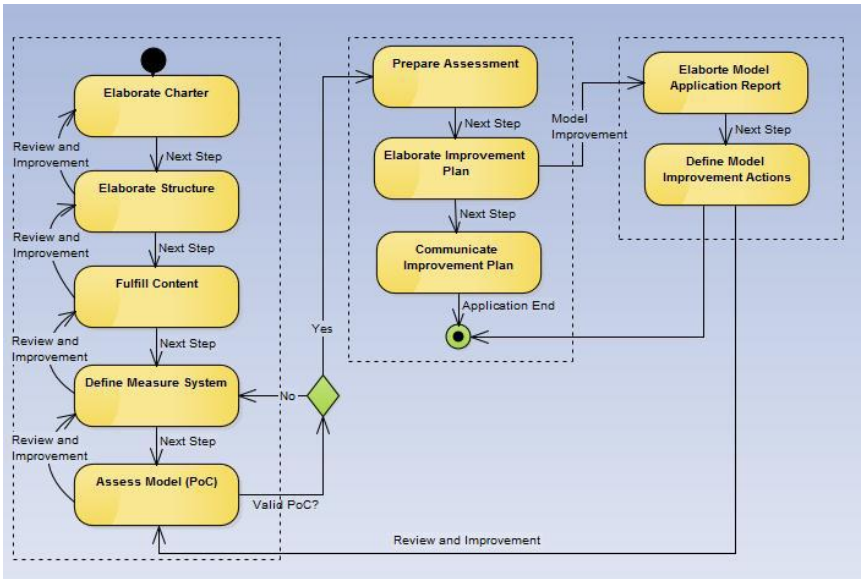

Figure 1: MMDPSI process description

3.1 Block 1: Design

The first block presents the design stages.

3.1.1 Establish charter

The establishment of the charter is the first step in developing the maturity model. The Charter may mainly include: model denomination, studied area description, scope, model purpose, development strategy, success factors, requirements, and stakeholders.

3.1.2 Establish the structure

The aim is to structuring the concepts of maturity depending on the purpose and scope of the model to develop and also defining the architecture or the representation according to which the evaluation will be made. In contrast to the other approaches cited in the literature review the definition of architecture at the MMDPIS process takes into consideration the purpose and requirements of the model to be developed.

This architecture can be of type: (1) staged, (2) continuous or (3) Focus Area. The choice must be justified and documented.

The staged architecture is adapted when it is a question of estimating the global maturity of the organization with regard to a given activity. This choice is recommended for example in case of benchmarking study.

The objective of the continuous architecture is to evaluate domains or process according to predefined levels of evolution, called "levels of capacity ". This choice is recommended when it is question of making a comparative study between these domains in a perspective to prioritize improvement axes.

As for the third architecture "Focus Area", it defines control objectives specifically for each area of studied activity depending on its life cycle phase. It enables to take into account the interdependencies between these control objectives.

3.1.3 Fulfill the structure

This step begins by identifying the elements of the model according to the adopted structure.

The explanation of these elements can be based on different approaches. The choice of method depends on the context of the model development.

Indeed, the most common and recognized approach of the methods of maturity models development is the literature review along with interviews of experts in the field. This approach is complete for some items when needed, especially for complex or new areas by exploratory methods such as Delphi technique, Focus group or case study.

The elements to be defined for all the types of structures are:

- Axes and elements of evaluation.
- Domains and groups of domain: the identified domains must be mutually exclusive and collectively exhaustive. The link Domain/Group of domain can be established according to a Top-Down or Button-up approach according to the context of model development.
- Objectives of control: for every domain, define the objectives of control.

Specific elements of each structure are:

- Maturity levels for staged architecture: define the maturity levels of the model and control objectives required for each domain to reach a given level.
- The capacity levels for continue architecture: define the capacity levels and control objectives required for each domain to reach a given capacity level.

The interdependencies and ranks of control objectives (CO) for FA architecture: define for each control objective a rank and dependencies on other control objectives (1).

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)

- These two elements are used to determine the maturity matrix and define maturity levels.

3.1.4 Defining the measurement system

In this stage are defined the elements of the measurement system:

- Elements of control: for every control objective define the corresponding control elements,
- Method and evaluation tools: it is necessary to define the method according to which the evaluation will be made and which tools to use for the collection of the measures and their exploitation,
- Evaluation Team: the human element is central to the measurement system. It is important at this stage to identify the requirements for this element or detail them if they are already identified in the model charter. These requirements may be under three aspects: skill, function and behavior. The latter can result in motivation, commitment and adherence to continuous improvement project.

3.1.5 Evaluate the model (PoC: Proof of Concept)

The purpose of this evaluation is to check whether the model designed meets the predefined requirements. Evaluation can be done through the progress of a case study example.

If the evaluation is satisfactory, the maturity model developed is implemented. Otherwise, a second iteration is started. The recovery was made from the stage representing the source of the problem or dissatisfaction.

3.2 Block 2: Implementation

The second block guides the implementation of the designed maturity model.

3.2.1 Prepare evaluation

The proposed evaluation process involves the following steps:

- Constitution of the evaluation team: It consists on constituting the team of evaluation according to the requirements predefined in the charter and the measurement system. The participation in this exercise must be accepted without additional or hidden responsibility for the evaluation team. The communication and the raising awareness of the team are important. A Quiz can help to do this and also to measure the adhesion of the team before beginning the evaluation.
- Define IS to evaluate: At this stage, we have to define the list of IS to evaluate. For each IS, it's important to define the corresponding life cycle phases and calculate the weight reflecting its importance in organism. We propose to calculate the weight based on three elements: (1) consumption of the cost, (2) consumption of the load, and (3) contribution to the strategy. Table 2 provides a calculation example of this weight. Column 1 provides the name of IS. Column 2 gives the rate of annual consumption compared to the total annual load. Column 3 shows the annual rate of consumption relative to the overall annual cost. Columns 4 to n describe the IS contributions in organization strategic objectives (SO). This qualification is made on a qualitative scale to which corresponds a quantitative scale: F: Strong 3, M: Medium 2 and Fb: Low 1. The first part of the column n+1 calculates the contribution according to predefined quantitative scale (2). The second part of this column gives the contribution in the form of rate with regard to the global contribution (for example for IS 1 is equal to 67% = 6 / (3 + 6)). The last column n + 2 is dedicated to the calculation of the overall weight of the IS based on the three elements previously defined: load consumption, consumption cost and contribution in the strategy. This weight is given by the formula (3).

$$\textit{Contribution} = [(3 * F\ \textit{value}) + (2 \times \textit{number M}) + (1 \times \textit{number Fb})] \quad (2)$$

*(for example for IS 1 is equal to 3 * 2 = 6)*

$$\textit{Weight} = (\textit{Val\_col 2+ Cal\_col3 + Val\_part2 (Col n+1)})\ (IS) / \textit{Total}\ (\textit{Val\_col 2+ Cal\_col3 + Val\_part2(Col n+1)})(\textit{all IS}). \quad (3)$$

Table 2: Example of calculating of the IS weight

IS	load Cons.	ost Cons.	Col.4S.O	...	Col.n S.O.	Col.n+1 Cont. S.O.		Col.n+2 weight IS
IS 1	25%	40%	F		F	6	67%	44%
IS 2	75%	60%			F	3	33%	56%

3.2.2 Establish an improvement plan

An evaluation plan depends on the adopted evaluation system. However, it usually contains: sessions of presentation and explanation of the model/ system evaluation tools, evaluation Workshops and outcomes discussion sessions.

The development of the improvement plan first requires an analysis of assessment results.

Once this analysis made, a list of the scenarios of improvement is established. These scenarios represent the possible paths of improvement. The person responsible for implementing the maturity model should select the most optimal path answering the objectives and constraints of the organism. Optimization paths for improvement may require the definition of the elements of calculating the improvement effort. He can involve in particular the knowledge of the cost and the load estimated as well as of the impact of implementation of the improvement actions.

3.2.3 Communicate the improvement plan

The improvement plan should be communicated to all stakeholders in an objective of validation, implementation and monitoring of improvement actions.

3.3 Block 3: continuous improvement

The third block is dedicated to the model continuous improvement. It is a question of defining the improvement actions of the developed model following its implementation.

- Develop the application report: This report serves to register reports and remarks resulting from the phase of implementation.
- Define the model improvement actions: it can give rise to a new iteration for its development.

4 Design of ISR3M Model

4.1 Elaboration of the model charter

Charter is constituted of following elements:

- **Denomination and studied area**: the model is called ISR3M (Information Systems Risk Management maturity model) and it is developed for the evaluation of IS risk management.
- **Scope**: domains concerned by the ISR3M model both in research and in practice are the risk management and the information systems. The definition adopted for the IS is that of a special case of work system [31]. The elements to be considered in the study of such systems are: participants, information, technology, processes, products and services, customers, infrastructure, environment and strategy. As for the risk management device, we adopt the ISO 31000 Framework [32] with the generic management cycle proposed by Sienou [33]. 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 [33], (2) the cycle of management preserves its iterative character, but no longer requires synchronization of all stages with a monitoring phase [33], and (3) Treatment may be the cause of a new iteration process [33].

- **Model purpose**: the objective of the ISR3M model is assessing IS risk management. The development of this model should provide answers to the above problem 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 avenues 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.
- **Development strategy**: it is a question of developing a new IS risk management maturity model using the MMDPIS process [5].
- **Success factors**: success factors of ISR3M model concern mainly: (1) taking into account the theoretical aspects of the concerned areas especially information and risk management systems, (2) involvement of stakeholders, and (3) simplicity and ease of implementation.
- **Application scope**: given the nature of the area studied, the application of ISR3M model concerns the whole organism.
- Requirements: the proposed requirements are the comparison criteria of maturity models presented in second section: c1: Genericity, c2: Independence of application context, c3: adaptability, c4: transparency, c5: plan improvement, c6: Theoretical basis and c7: need Adequacy (IS RM).
- **Stakeholders**: it involves target audience (IS risk management device evaluators, auditors...), implementation responsible (IS risk management managers), and respondents and interviewees (risk managers, IS project managers.., etc).

4.2 Establishment of the structure

The ISR3M model is structured along two dimensions. The first dimension includes evaluated activities. It is a question of risk management activities. The second dimension represents the aspects under which these activities are evaluated. It is a question of evaluation axes and elements related to an IS defined as a WS.

The maturity assessment is made according to the architecture "Focus Area". 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 ISR3M model. Indeed, it defines small evolutionary steps thus making improvement easier, less risky and less costly. The road improvement is clearer.

The choice is also justified by taking into account the interdependence of the control objectives which is an important characteristic of the risk management business.

4.3 Populate the structure

4.3.1 Determination of the axes and elements of evaluation

The areas of assessment are the elements of the IS defined as WS [31]. 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 [31], (2) the application of the theory RBV (Resource Based-view) [34] on IS

defined as WS considering both dynamic resources such as skills, as static as the technical infrastructure, (3) the IS risk factors [35], and (4) interviews with IS experts.

Table 3 lists the evaluation elements for each component.

Table 3: IS 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	Customer	Needs
	Strategic profile		Satisfaction
Participants	Competence		Competence
	Cooperation		Cooperation
	stability		

4.3.2 Definition of domains and domains groups

The areas adopted for ISR3M 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 4. 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 4: ISR3M 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
	Implementation of the treatment plan
	Monitoring and review
Recording	Recording

4.3.3 Determination of 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

4.3.4 Determining the position of the objectives control in the maturity matrix

The position of the control objectives 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 2.

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 2: Positioning matrix

4.4 Definition of evaluation system

4.4.1 Definition of control elements

In order to build this system, we use an approach based on the principle of the method GQM (Goal-Question-Metric) [36]. 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 ISR3M model control elements, are specifically defined for each control objective from its requirements.

Table 5 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 5: 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."

4.4.2 Method and Assessment Tool

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 domain " 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 (4).

$$Measure\_EC\ (Axe\_Eval) = Round\ [mean\ (Mesure\_EC\ (Elt\_Eval\ i) \times Valeur\_Applicable\ (Elt\_Eval\ i))]; 1 <= i <= number\ of\ assessment\ items\ in\ Axe\_Eval \quad (4)$$

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 (5). 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.

$$Measure\ (EC) = Round\ [Sum\ (weight\ (Axe\_Eval\ j) \times Mesure\_EC\ (Axe\_Eval\ j))]; 1 <= j <= 9\ (number\ of\ evaluation\ axes = 9) \quad (5)$$

The measure of a control objective is "yes" if all the corresponding questions are "yes" (value 1) and "no" (value 0) otherwise (6).

$$Measure\ (OC) = product\ (Measure\ (EC\ i)); 1 <= i <= number\ of\ EC\ in\ OC \quad (6)$$

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 3: Example of maturity matrix

4.4.3 Definition of the evaluation team

The evaluation team should be constituted mainly from:

- Responsible of implementation: he can involve for example auditors or external consultants.
- People asked: it is mainly about risk managers, IS project managers and business managers.

4.4.4 Model evaluation

The evaluation can be realized through the application of the designed model on a pilot information system. It has for objective to test the applicability of the proposed version.

We applied the model in three iterations on three different IS. Adjustments and adaptations concern including control elements, dependencies and positioning control objectives of the various fields in the maturity matrix.

5 Implementation

5.1 Evaluation approach

The implementation begins with the definition of the team of evaluation and their raising awareness with regard the importance and to the added value of the work to be made.

A working session was then held with the constituted team. Its primary purpose is to explain to members the main concepts used in the ISR3M model. These include the information system definition and the risk management process. A second objective is to present the evaluation system.

The evaluation team has the task of describing the IS object of the valuation. This description requires the definition of four main elements for each SI: (1) the nine elements of the WSF, (2) the weight of these elements in relation to the different phases of the IS life cycle, (3) IS current phase over its life cycle, and (4) the IS weight in relation to the management of global IS risks. This weight can be calculated using the method proposed by the MMDPIS process (3).

The questionnaire is informed by the evaluation team. A workshop is provided later to discuss the answers and finalize the results. This workshop allows the administration of the questionnaire via the "face-to-face." This approach allows for more reliable and less confused answers.

5.2 Elaboration of improvement plan

5.2.1 Analysis of evaluation outcome

The results of the evaluation are maturity matrix for each IS and an overall maturity matrix. The latter is established and analyzed in three visions. The first is a "pessimistic" vision involving the minimum control objectives per domain. Through this vision are located the most defective areas in risk management. The second is an "optimistic" vision. It brings maximum control objectives per domain. This allows to know the most advanced areas in risk management and to create a positive synergy between all the IS. The third vision provide the overall maturity of IS risk management. It is obtained through a weighted average of different IS maturity matrices.

The design of a pivot table allows to conduct an analysis of the evaluation results (by IS, control objective, level of maturity, etc.) according to the need for the decision-makers.

5.2.2 Determination of the improvement strategy

To define the improvement strategy, the organism defines at first the approach of improvement. The latter can be made according to two approaches. The first one is an approach " top - down ". In this case, the target is defined at the level of the global maturity matrix and then declined on the maturity matrices of the various IS.

The second approach is an approach "button-up". This approach allows the organism to define the target maturities at the level of every IS. The improvement of the global maturity is the consolidation of the improvements of the various IS.

Secondly the organism defines the desired way of improvement: by maturity level target or control objective target.

If the organism decides to improve his IS risk management maturity towards a given maturity level then all the objectives of control placed before this level must be reached. The actions to be realized are clear.

If the organism decides to improve the maturity by control objectives target, it must ensure that the prerequisites of target control objectives are checked. These are mainly related to dependency constraints.

To guide the selection and implementation of the treatment strategy, we propose two algorithms: the first, called "prerequisite-way", is dedicated to the definition of the prerequisites to achieve a given target.

The second called "improvement declination» define from a global target control objective the control objectives by IS to achieve with optimizing effort.

Table 6 presents a summary of the proposed improvement strategies.

Table 6: Improvement strategies.

Improvement strategy	Improvement approach	Target definition	Proposed algorithm
Top-Down by maturity level	Top-Down	By maturity level	Prerequisite-way Improvement declination
Top-Down by control objective		By control objective	Prerequisite-way Improvement declination
Buttom-up by maturity level	Buttom-Up	By maturity level	Prerequisite-way
Buttom-up by control objective		By control objective	Prerequisite-way

5.2.3 Elaboration of improvement plan

Once the improvement strategy elaborated, the plan of improvement is established. The latter is formed by the necessary actions for the achievement of the target control objectives. These actions arise from those proposed for the implementation of the control objectives. The treatment plan has to specify the responsible and the schedule of implementation as well as monitoring milestones.

5.2.4 Communicate the improvement plan

Improvement plan is communicated to all stakeholders for monitoring and implementation.

6 ISR3M Evaluation

The evaluation of the model is realized according to two axes. The first one concerns the criteria proposed in second section (table 7). The second axis concerns a naturalistic evaluation of the model. It will be presented in an upcoming paper.

Table 7: Evaluation of ISR3M

Criteria	Evaluation
C1: Genericity: the proposed solution should be generic viewpoint processes and IS risk management concepts,	The process on which is based the proposed model is the one of the standard ISO 31000 which is generic viewpoint process and RM concepts.
C2: independence of the context of application: the solution must be applicable in all the contexts and the business sectors,	The model can be applied to any IS in all contexts and sectors.
C3: Adaptability: The solution must take into account the specificities of the area studied,	A "Applicable" parameter is introduced during the evaluation at the level of every element of evaluation. This parameter allows to specify if each of the latter is considered or not according to the context of IS or of the organism.
C4: transparency: the solution has to insure the documentation and the traceability of the measures of maturity,	Evaluation system as well as the documents registered for every version of the model insures the traceability of the measures.
C5: plan improvement: does the model assist its	The model assists its users in the definition of the strategy

Criteria	Evaluation
users in the definition of a improvement plan?	and the improvement ways of both proposed algorithms.
C6: theoretical Basis: does the model base itself on the theoretical aspect of the domain studied for the measure of the maturity?	The model ISR3M is effectively based on the theoretical aspect of the various domains of its scope through the detailed study and the effort dedicated to the corresponding literature specially in information system and risk management.
C7: adequacy to needs (IS risk management): is the model adapted to the IS risk management?	The model is developed for the evaluation of the IS risk management.

7 Conclusion

IS risk management is becoming increasingly widespread. The evaluation of this discipline through maturity models in a perspective of continuous improvement is a guarantee of the preservation of its value as a profit center. A series of works related to the assessment of this discipline exist but have limitations in scope and design. Indeed, on the one hand, the existing maturity models deal only with aspects related to IT. On the other hand, these models have conceptual limitations such as: (1) lack of satisfactory answers to the implementation of the improvement actions, (2) the certainty falsified given to decision makers, (3) poor base theoretical, (4) inadequate model validity tests, (5) failure to fit the specific needs of the areas studied, and (6) the high level of formality. The absence of documentation and transparency as for valuation methods are added to these limits.

The solution proposed in this article is the ISR3M model. This maturity model is dedicated to the evaluation of the IS risk management. It is developed according to the MMDPIS process [5] so as to address the problem stated above. Its evaluation shows compliance with pre-established requirements.

The presentation of the implementation results of ISR3M model on an actual case study is planned in future work.

REFERENCES

[1] Salvati, D. (2008). *Management of Information System Risks.* Zurich: University of Zurich.

[2] Lei, Y. (2011). Minimizing the Cost of Risk with Simulation Optimization Technique. *Risk Management and Insurance Review, 14*(1), 121-144.

[3] Zhang, Y. (2009, May). A Study on Risk Cost Management. *International Journal of Business and Management, 4*(5), 145-148.

[4] Bronet, V. (2006, Septembre). *Amélioration de la performance industrielle à partir d'un processus Référent Déploiement inter entreprises de bonnes pratiques.* Savoie: Université de Savoie.

[5] El maallam, M and Kriouile, A, (2014). A generic process for the development and the implementation of IS maturity models. International Journal of Computer Science Issues (IJCSI), 11(6), pp. 34-42.

[6] Poeppelbuss, J., Niehaves, B., Simons, A., and 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.

[7] Pfeffer, J., and Sutton, R. I. (1999). Knowing what to do is not enough: turning knowledge into action. *California Management Review, 42*(1), 83-108.

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

[9] Mettler, T. (2011). Maturity assessment models: a design science research approach. *International Journal of Society Systems Science, 3*(1/2), 81-98.

[10] Mettler, T., and Rohner, P. (2009). Situational maturity models as instrumental artifacts for organizational design. *4th International Conference on Design Science Research in Information Systems and Technology DESRIST'09. 22*, pp. 1-9. New York, NY, USA: ACM.

[11] Benbasat, I., Dexter, A. S., Drury, D. H., and Goldstein, R. C. (1984, May). A critque of the stage hypothesis: theory and empirical evidence. *Communications of the ACM, 27*(5), 476-485.

[12] De bruin, T., Freeze, R., Kulkami, U., and Rosemann, M. (2005). Understanding the Main Phases of Developing a Maturity Assessment Model. *Australasian (ACIS).* Autralie, Sydney.

[13] King, J. L., and Kraemer, K. L. (1984, May). Evolution and organizational information systems: an assessment of Nolan's stage model. *Communications of the ACM, 27*(5), 466-475.

[14] McCormack, K., Willems, J., Bergh, v. d., Deschoolmeester, D., Willaert, P., Stemberger, M. I., et al. (2009). A global investigation of key turning points in business process maturity. *Business Process Management Journal, 15*(5), 792-815.

[15] Biberoglu, E., and Haddad, H. (2002, Decembre). A survey of industrial experiences with CMM and the teaching of CMM practices. *Journal of Computing Sciences in Colleges, 18*(2), 143-152.

[16] Montoya-Weiss, M. M., and Calantone, R. (1994). Determinants of New Product Performance: A Review and Meta-Analysis. *Journal of Product Innovation Management, 11*(5), 397-417.

[17] Becker, J., Knackstedt, R., and Pöppelbuß, J. (2009). Developing Maturity Models for IT Management – A Procedure Model and its Application. *Business & Information Systems Engineering (BISE), 1*(3), 213-222.

[18] Becker, J., Niehaves, B., Pöppelbuß, J., and Simons, A. (2010). Maturity Models in IS Research. *18th European Conference on Information Systems (ECIS 2010).* Pretoria, South Africa.

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

[20] Dey, A. K. (2000). *Providing architectural support for building context-aware applications.* Atlanta, GA, USA: Georgia Institute of Technology.

[21] Herbsleb, J. D., and 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.

[22] Teo, T. S., and King, W. R. (1997). Integration between Business Planning and Information Systems Planning: An Evolutionary-Contingency Perspective. *Journal of Management Information Systems, 14*(1), 185-214.

[23] Hillson, D. A. (1997). Towards a risk maturity model. *The International Journal of Project and Business Risk Management, 1*(1), 35-45.

[24] Hopkinson, M. (2011). *The Project Risk Maturity Model: Measuring and improving risk management capability.* Gower.

[25] Ren, Y. T., and Yeo, K. T. (2009). Risk management capability maturity model for complex product systems (CoPS) projects. *Systems Engineering, 12*(1), 275-294.

[26] Saito, O., Matsui, T., and Morioka, T. (2007). Organizational Risk Management Maturity Model and Assessment Tool Designed for High-hazard Industries. *International Symposium on Symbiotic Nuclear Power Systems for 21st Century (ISSNP)*, 42-47.

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

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

[29] Mayer, J., and 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.

[30] ISACA. (2010). *RISK IT Framework.*

[31] Alter, S., and 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.

[32] ISO. *ISO 31000:2009 Risk Management. Principles and Guidelines on Implementation.* Tech. rep.

[33] 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.

[34] Wade, M., and 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.

[35] Alter, S., and 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.

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

