A Model of Maturity for IS Risk Management Case Study

Mina Elmaallam[1] & Abdelaziz Kriouile[1]

[1] ENSIAS, Avenue Mohammed Ben Abdallah Regragui, Madinat Al Irfane, Agdal Rabat, Maroc

Correspondence: Mina Elmaallam, ENSIAS, Avenue Mohammed Ben Abdallah Regragui, Madinat Al Irfane, BP 713, Agdal Rabat, Maroc. E-mail: elmaallam@gmail.com

Received: January 11, 2012 Accepted: February 20, 2012 Online Published: May 1, 2012

doi:10.5539/cis.v5n3p97 URL: http://dx.doi.org/10.5539/cis.v5n3p97

Abstract

This paper is a continuation of our first paper dedicated to the presentation of the maturity model for information system (IS) risk management (RM). Its objective is to place the model proposed in the first paper on a case study by the assessment of the maturity of risk management for an IS-CRM (IS dedicated to customer relationship management (CRM)). The sequence of the model requires prior definition of an evaluation system incorporating the setting, the measurement and consolidation methods. In our case study we have gone through four steps: definition of studied components, evaluation of control objectives, calculate the maturity levels for each activity of the RM process and calculate the RM process maturity.

Keywords: information system, risk, risk management, model of maturity, life cycle

1. Introduction

The aim of an IS risk management process is to ensure the achievement of its objectives and guard it against any threat. However, this goal can only be achieved if the process is monitored and controlled. For this, we must establish a system of measuring well-defined since we can only control what we can measure. Hence the interest to develop a maturity model of risk management information systems. This was the aim of our first paper (Elmaallam & Kriouile, 2011).

For this paper, we aim to test the applicability of the model proposed in the first paper and devoted to assess the IS risk management maturity (Elmaallam & Kriouile, 2011). This assessment concerns only the case of a single information system. The maturity of a global information system will be evaluated in futures case studies.

The paper has five sections. After this introduction, the second section reminds the IS definition on witch our model is based.

The third section of this paper points out the proposed model for assessing the IS risk management maturity.

The fourth section presents the case study proposed for the application of the model designed.

In the fifth section, we conclude our paper and present the prospects of this work.

2. Information Systems: Definition

There are several definitions of an information system (Carvalho, 2000). In our study, we adopted the definition of the IS as a work system (Alter, 2008). We opted for this definition since it clearly identifies the components of an IS and eliminates any confusion with the IT systems.

A work system is a system 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).

The components of a work system are illustrated in the Figure 1.

An IS 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).

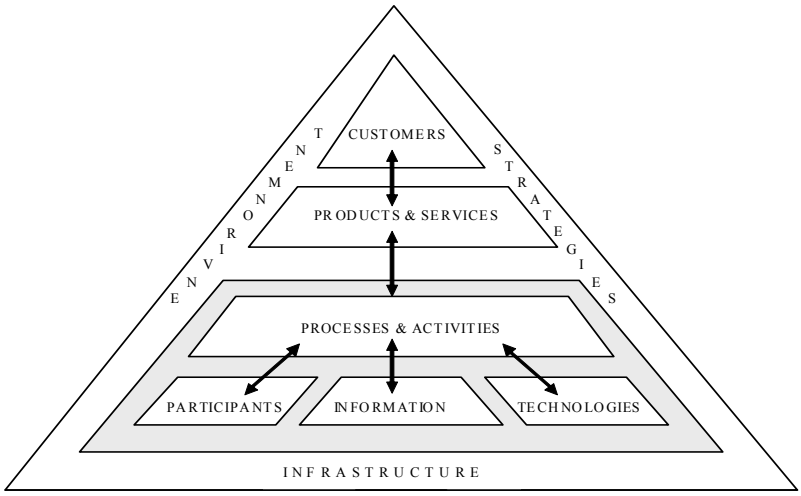

Figure 1. The work system framework (Alter, 2002)

3. IS Risk Management: Definitions and Process

3.1 Definitions

A risk is the possibility of an event occurrence that will impact the objectives achievement. Risk is measured in terms of consequences and probabilities (IFACI, 2009).

For the company, as an economic unit, the risks are divided into five categories (Akim, 2008):

- Market risk: results in exposure to fluctuations in market parameters such as interest rate risk, exchange rate risk (Akim, 2008).

- Credit risk: investor's risk of loss arising from a borrower who does not make payments as promised (Akim, 2008)

- Operational risk: represents threats that an organization faces in managing daily activities (Akim, 2008).

- Political, regulatory, and legal risks: those risks condition the immediate external environment of the company and set or change it competitive position (Akim, 2008).

- Liquidity risk: the risk of lack of funds at any time to meet the immediate payment of its commitments (Akim, 2008).

IS risks are operational risks as long as they directly affect the company activity at any stage of the IS life cycle, from IS initiation until IS exploitation and maintenance (Goldstein, Benaroch, & Chernobal, 2008).

The conceptualization of risk is the way in which risk is expressed and formulated in elements allowing its management. The literature of IS risk uses several risk conceptualizations which can be classified in three categories (Alter & Sherer, 2004):

Components of the risks or types of negative results: The first risks conceptualization identifies different types of negative outcomes (Alter & Sherer, 2004). (Example: project risks, functional risks, politics risks, security risks)

Typical risk factors: The second risks conceptualization is the risk factors such as the project size, the use of new software, or the hostile employees (Alter & Sherer, 2004).

Probability of the negative results: The third risks conceptualization considers risk as probability of negative results. It is measured as a probability distribution of negative results, often balanced by financial losses (Alter & Sherer, 2004).

3.2 Risk Management Process

Risk management is a process, effected by an entity's board of directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risks to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives (IFACI, PriceWaterhouse-Coopers & Landwell, 2005).

The study of literature indicates the non existence of a process dedicated to IS risk management. There are

processes and methods used form managing risks of some IS parts: information security (ISO 27005 process, EBIOS method), IS project management (PMBOK) and IT governance (PO09 COBIT process). Nevertheless, we believe that the risk management process in ISO 31000 can be applied to many different disciplines including the area of IS risk management.

The risk management process according to ISO 31000 (ISO, 2009) has five main activities (Figure 2).

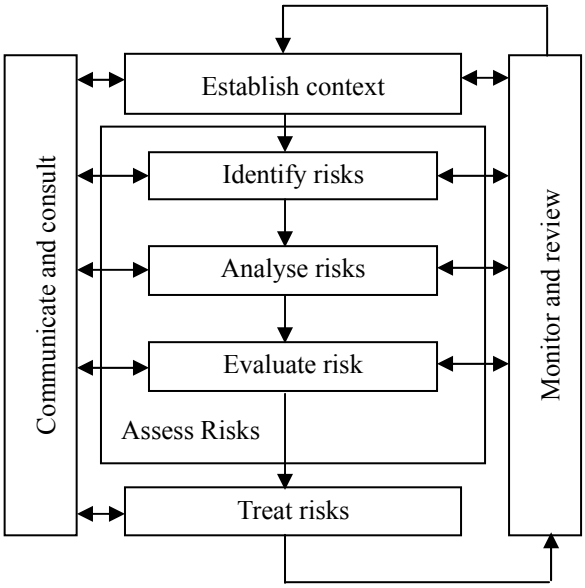

Figure 2. ISO 31000 Risk management process (ISO, 2009)

Communication: A plan of communication must be elaborated and communicated, in each phase and every update, since the creation of the risk management process.

Establishment of the context: In this phase the organization defines the context in witch the risk management process will be elaborated and followed. This contexte specifies in a clear way its objectives, the internal and external parameters to take into account in the risk management, and identifies the field of application, the scope and the risk criteria for the rest of the process.

Risk assessment: Risk assessment is the overall process of identification, analysis and risk evaluation.

Risk treatment: Risk treatment is the methods and resources used to control it. It includes the implementation of measures to control risks and a sub-processing activity of the residual or so-called business risk acceptance (ISO, 2008).

Monitoring and review: Check, supervision, critical observation or determination of the state to identify continuously changes with regard to the required or expected level of performance (ISO, 2009).

4. The Proposed Model of Maturity for Assessing the IS Risk Management

4.1 Model Overview

Our maturity model of IS risk management is based on the results of our study on the IS definition, the process of risk management and maturity models. To define this model, we have selected the following elements (Elmaallam & Kriouile, 2011):

- The process of risk management (five activities)
- The life cycle of an IS
- The nine constituents of an IS
- The levels of maturity

Our model proposes the following approach for assessing the maturity of IS risk management of a company (Elmaallam & Kriouile, 2011):

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

For all IS:

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

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

Our model can be represented under the matrix shape mentioned in the Table 1 (Elmaallam & Kriouile, 2011).

Table 1. Illustration of IS risk management maturity model

		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***
IS - 2 (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.2	***ML-A1/IS.2***	***ML-A2/IS.2***	***ML-A3/IS.2***	***ML-A4/IS.2***	***ML-A5/IS.2***	***ML-PR/IS.2***
. ..							
IS - n (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.n	***ML-A1/IS.n***	***ML-A2/IS.n***	***ML-A3/IS.n***	***ML-A4/IS.n***	***ML-A5/IS.n***	***ML-PR/IS.n***
All IS		**ML-A1**	**ML-A2**	**ML-A3**	**ML-A4**	**ML-A5**	**ML-PR**

The model matrix lists in lines all IS for the related company (IS - 1, IS - 2, IS - n). Then, every IS is determined under its nine constituents (C1, C2, C3, C4, C4, C5, C6, C7, C8, C9). For each IS, the line "IS" represents the whole IS.

The model matrix lists in columns the five activities of the risk management process (A1, A2, A3, A4, A5). The last column "PR" represents the whole process (Elmaallam & Kriouile, 2011).

For each IS:

- The value “ML-Ai/Cj” of the pair (Ai, Cj) is the maturity level of Ai activity applied to the Cj constituent
- The value "“ML-Ai/SI.k” of the pair (Ai, IS.k) is the maturity level of the Ai activity applied to the IS-k
- The value “ML-PR/Cj” of the pair (PR, Cj) is the maturity level of the process applied to the Cj constituent
- The value “ML-PR/ IS.k” of the pair (PR, IS.k) is the maturity level of the process applied to the IS-k

For all IS:

- The value “ML-Ai” is the maturity level of the Ai activity applied to the all IS
- The value “ML-PR” is the maturity level of the process applied to the all IS

In the rest of the paper we define the levels of maturity as well as the elements used for their evaluation. However, we are going to consider the following hypotheses (Elmaallam & Kriouile, 2011):

- Only one IS to estimate
- The phases of the life cycle have no impact on the control elements and on the control objectives

4.2 Maturity Levels

The chosen model has five levels of maturity. This choice is justified by the studied literature. Indeed, most of the selected models are structured at levels that number varies between four and five levels according to consider or not the risk management existence in the studied organization (Mayer & Fagundes, 2009). The five levels proposed are:

Level 1, initial: The work is based on individual initiatives. No methodology or procedure (based on the best practices) 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.

4.3 Elements of Control

The elements of control are a practical translation of the IS constituents that will be the evaluation subject of the risk management maturity (Ciorciari & Blattner, 2008). Table 2 gives the list that we propose for control elements. Those control elements are defined through a study of risk factors (Alter & Sherer, 2004) related to each IS constituent.

Table 2. Description of the control elements for the IS constituents

Components	Control elements
Participants	- Skill and expertise - Degree of cooperation of the participants - Turn over - Availability of the staff - Mode of management - Communication

	-	Culture of the participants
Technologies	-	Novelty of the technologies
	-	Opening of the technologies
	-	Performances of machines
	-	Requirements of networks / telecommunication
	-	Adequacy of the software / platform used
Information	-	Information security: availability, integrity, confidentiality and traceability
	-	Relevance of the information
Work practices	-	Formalization of the processes / procedures
	-	Adequacy of business procedures
	-	Updating of the procedures
	-	Dependence of the computer systems
	-	Interdependence of the processes / procedures
	-	Link with the organization
	-	Needs it competences
Products & services	-	Correspondence of the product at the need
	-	Quality of the product and service
	-	Exploitation of the product
Customers	-	Category of the customers
	-	Level of precision of the needs of the customers
	-	Level of requirement of the customers
	-	Customer satisfaction
	-	Definition of the scope
	-	Skill / training of the customers
	-	Culture of the customers
	-	Cooperation of the customers
Infrastructure	-	Organization
	-	Software, Hardware, equipment
	-	Telecom infrastructure
	-	Help desk
Environment	-	Stability of the market (resources, cost, IT)
	-	Relation with the stakeholders
	-	Natural events
	-	Security of the persons and the properties
	-	Cultural elements
Strategies	-	Alignment on the objectives strategic
	-	Strategic resources
	-	Contribution to the strategy

ISSN 1913-8989 E-ISSN 1913-8997

4.4 Control Objectives

A control objective is defined as the declaration of a purpose or an aimed result, through the implementation of controls in an activity given by the process of risk management. The controls are the policies, the procedures, the practices and the organizational structures, conceived to supply a reasonable guarantee that the objectives of the organization will be reached and that the unwanted events will be avoided or deleted and corrected (ISO, 2005).

Control objectives define the criteria to be met by controlled operations. These criteria apply to both basic business objectives and its integration into a continuous improvement process through audit and return on experience.

We define in the following sub-sections the control objectives proposed for each activity of the risk management process.

4.4.1 Objectives of Control of the Activity “Establishment of the Context”

The purpose of this activity is to define the context in which will be deployed the process of risk management. The context must include the elements to be taken into consideration such as: policy, organization, constraints, assumptions and methods and criteria for risk management.

To answer this purpose, we propose the following control objectives:

- EC.1. Develop an identification sheet of IS studied,
- EC.2. Define the objectives of the process of risk management,
- EC.3. Define an normalized method for the definition of the context,
- EC.4. Define a method of appreciation of the risks,
- EC.5. Define a method of treatment of the risks,
- EC.6. Define a method for the evaluation of the efficiency of plans treatment,
- EC.7. Define a plan of communication,
- EC.8. Define a procedure of review and surveillance,
- EC.9. Define the level of tolerance or acceptance of the risks,
- EC.10. Collect and store information necessary to evaluate the activity,
- EC.11. Audit the activity,
- EC.12. Define an action plan of adjustment and improvement of the activity.

4.4.2 Objectives of Control of the Activity “Risk Assessment”

The purpose of this activity is the identification, analysis and risk assessment. The identification will result in an exhaustive list of risks via the definition of assets to protect, their vulnerability and the threats they are exposed. The analysis is used to filter the identified risks to keep only those most relevant and appropriate to the context defined in the activity “Establishment of the context”. The assessment is used to measure the criticality of the risks to classify them according to the thresholds defined at the activity "definition of context."

To answer this purpose, we propose the following control objectives:

- AP.1. Identify the risks
- AP.2. Analyze the risks
- AP.3. Estimate the risks
- AP.4. Apply the methodology of appreciation of the risks defined in the context
- AP.5. Automate the process of analysis/evaluation
- AP.6. Collect and store information necessary to evaluate the activity
- AP.7. Audit the activity
- AP.8. Define an action plan of adjustment and improvement of the activity

4.4.3 Objectives of Control of the Activity “Risk Treatment”

The purpose of this activity is to treat the risks identified after completion of the activity of risk assessment. It involves two stages: "the implementation of the treatment plan" and "acceptance of risk." In the first phase, the goal is to define treatment strategies depending on the context of the risks already identified. The second phase is

used to define the residual risks accepted. These risks are addressed and responding to acceptance criteria defined in the context.

To answer this purpose, we propose the following control objectives:

- TR.1. Choose the appropriate options of treatment of lists of the options proposed in the context
- TR.2. Draw up a plan of treatment of the risks
- TR.3. Evaluate the efficiency of the plan of treatment
- TR.4. Apply the method of treatment defined in the context
- TR.5. Apply the method of evaluation of the efficiency of the treatment plan
- TR.6 Collect and store information necessary to evaluate the activity
- TR.7. Audit the activity
- TR.8. Define an action plan of adjustment and improvement of the activity

4.4.4 Objectives of Control of the Activity “Communication”

The purpose of this activity is to define and monitor the plan for risk communication. The plan includes staff awareness of the importance of the discipline of risk management, and communication about risk management activities (mapping, treatment plan, monitoring indicators of risk, etc.).

To answer this purpose, we propose the following control objectives:

- CR.1. Implement actions, of awareness and communication
- CR.2. implement the communication plan defined in the context
- CR.3. Collect and store information necessary to evaluate the activity
- CR.4. Audit the activity
- CR.5. Define an action plan of adjustment and improvement of the activity

4.4.5 Objectives of Control of the Activity “Monitoring and Review”

The purpose of this activity is to ensure that the process remains relevant and effective, and is part of a continuous improvement process. For this, we must define indicators of risk control, and close monitoring of risk treatment plan. It should also set SMART goals for the process and measure their achievement through performance indicators defined.

To answer this purpose, we propose the following control objectives:

- SR.1. Monitor risk management indicators
- SR.2. Monitor the objectives of the process of risk management
- SR.3. Apply the procedure for reviewing and monitoring defined in the context
- SR.4. Collect and store information necessary to evaluate the activity
- SR.5. Audit the activity
- SR.6. Define an action plan of adjustment and improvement of the activity

4.5 Measure of the Maturity

4.5.1 Measure of an Element of Control by an Objective of Control

According to the proposed model, the measure of the maturity of the risk management of an information system will make towards the evaluation of the objectives of control sub - mentioned applied to elements defined for each IS component. The table 4 presents the control map for the various components. This evaluation will be made through a questionnaire and an echelon of measure.

4.5.2 Control Map

The control objectives are defined by an increasing level of requirement with respect to each activity process. The requirement level is aligned to the maturity level already defined. For example, for the activity "definition of the context," we believe that a minimum of items necessary to begin is to develop an identification sheet SI studied. A level of maturity maximal is able to submit this activity to the continuous improvement process through the exploitation and analysis of data collected on the deployment process. The Table 3 presents the control map for the various components.

Table 3. Control map

Activity	Level 1	Level 2	Level 3	Level 4	Level 5
Establish context	No control is implemented	EC.1, EC.2	EC.3, EC.4, EC.5, EC.6, EC.7, EC.8, EC.9	EC.10	EC.11, EC.12
Risk Assessment	No control is implemented	AP.1, AP.2, AP.3	AP.4	AP.5, AP.6	AP.7, AP8
Risk treatment	No control is implemented	TR.1, TR.2, TR.3	TR.4, TR.5	TR.6	TR.7, TR.8
Communication	No control is implemented	CR.1	CR.2	CR.3	CR.4, CR.5
Monitoring and review	No control is implemented	SR.1, SR.2	SR.3	SR.4	SR.5, SR.6

5. Case Study

5.1 Assessment System: Assumptions and Parameters

In this case study we unfold our model on a single information system. We also assume that the life cycle of the IS system studied does not influence the RM process maturity.

The maturity assessment involves the evaluation of control objectives on each control element for each component of the IS. To ensure flexibility of the evaluation system depends on environments in which IS studied evolves we introduced a parameter indicating whether a control element of a component is (value 1) or not (value 0) required. Thus, maturity measured for a component of an objective is the consolidation of control elements assessments weighted by the parameter value.

5.2 Case Study: Model Applied to the SI-CRM

- Definition of CRM IS

The model will be applied to a case of information system dedicated to customer relationship management (CRM Customer Relationship Management).

The Table 4 gives a description of the components of IS studied: IS-CRM.

Table 4. Description of IS-CRM studied

Component	Description
Infrastructure	- Customers reception space - Call center - Servers machines running applications software - Telephony
Strategies	- Customers satisfaction is a strategic objective - Availability of 24/24 and 7/7 - Offering online services to the customers
Environment	- The process approach established - To Satisfy the customers is a culture
Technologies	- CRM software - Queue management software - EDM (Electronic Document Management) - Web sites

Information	- Paper-based information - Computer-based information
Participants	- Responsible of customers - Tele-Advisors - IT Specialists - Process owner
Business process	- Customers relationship - Recovery - Career management - Payment
Products & services	- Update of the situation - Consultation of the situation - Certificate of pension
Customers	- Retired - Employers

- Assessment of the maturity level for each activity

Maturity evaluation of an activity involves the evaluation of control objectives in each control element for each component of the IS CRM. We define for each control objective three lines:

A line setting: used to define the control elements required for the evaluation of a component.

A line for evaluation: the box corresponding to a control element is set to 1 if the objective of control is applied at the control element and 0 otherwise.

A line of consolidation: Measuring the maturity level of a component is done by the consolidation of assessments of the control elements taking into account the values: parameter (line setting), evaluation (line for evaluation), and also a tolerance level. The latter value is beyond the measure of the goal of Control in activity is not zero and the value is rounded to 1.

An extract of maturity assessment of the establish context activity is given in Figure 3.

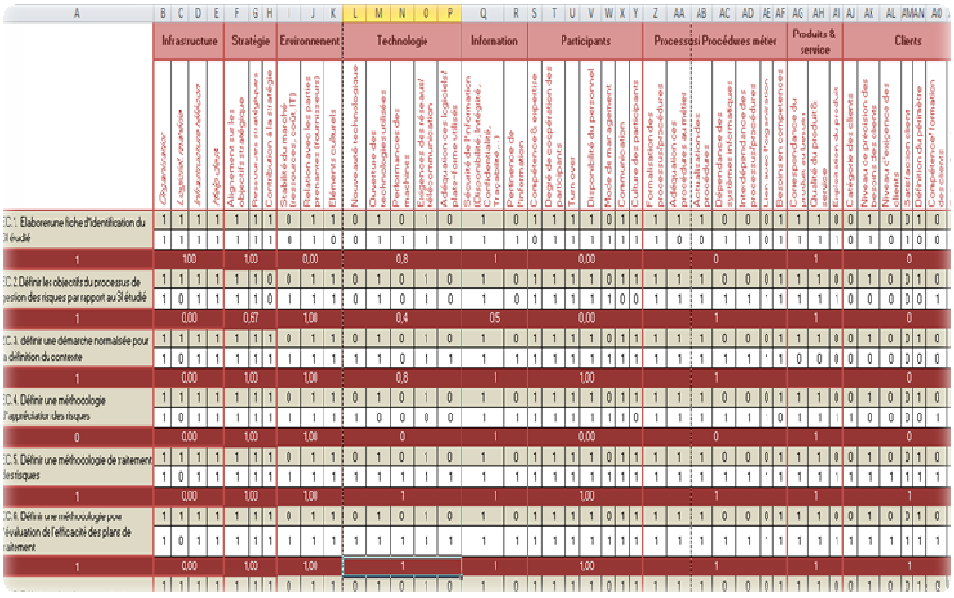

Figure 3. Extract of RM activity maturity assessment

- Control map

For each business process risk management, we evaluate the maturity by level, based on the consolidation measures defined in the previous step (assess the maturity level of each activity). The value given to each level is the result of "and" logical measures of control objectives define the level in question. The result of the control map is given in Table 5.

Table 5. Control map of IS-CRM studied

	Level 2	Level 3	Level 4	Level 5
Establishment of the context	EC1, EC2	EC.3, EC.4, EC.5, EC.6, EC.7, EC.8, EC.9	EC.10	EC.11, EC.12
Evaluation	1	0	1	1
Risk assessment	AP.1, AP.2, AP.3	AP.4	AP.5, AP.6	AP.7, AP8
Evaluation	1	0	1	0
Risk treatment	TR.1, TR.2, TR.3	TR.4, TR.5	TR.6	TR.7, TR.8
Evaluation	1	0	1	1
Communication	CR.1	CR.2	CR.3	CR.4, CR.5
Evaluation	1	0	1	0
Monitoring and review	SR.1, SR.2	SR.3	SR.4	SR.5, SR.6
Evaluation	1	1	0	1

- Measurement of maturity levels by activity

We then calculate the level of maturity for each activity of the RM process. The level of activity is the index of the last no-null level. For example, if we consider the activity "Establishing the context", the last level in which the measure of maturity is not null is level 2. The level of maturity given to the process of risk management is the minimum level measured for all its activities.

Table 6 gives the maturity levels calculate for the RM process and its activities.

Table 6. Maturity level per activity for the IS-CRM studied

Activity	Maturity level
Establishment of the context	2
Risk assessment	2
Risk treatment	2
Communication	2
Monitoring and review	3
Process	2

Figure 4 shows the RM process maturity levels.

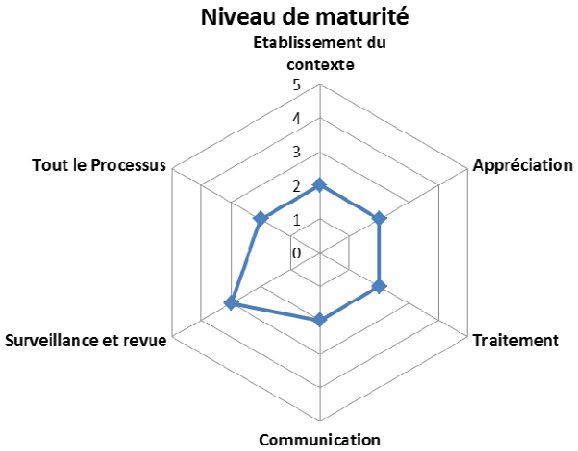

Figure 4. RM process maturity level for IS-CRM

6. Conclusion

We have presented in this paper the results of the case study of the model proposed to evaluate the maturity of IS risk management. Study was conducted with the assumption:

- The evolution of IS in its life cycle are not taken into account in assessing the maturity

- The study covers a single IS. The overall maturity of the global IS will be discussed in futures studies

This study has identified a few lines of thought around the proposed model such as:

- The completeness and adequacy of control elements

- The consolidation method for calculating assessments by activity and process

So our next research work will focus on extending the model to account for the life cycle of the IS into account the axes of reflection and improvement points raised in this case study.

References

Akim, A. (2008). *La gestion du risque opérationnel, application à la lutte contre la fraude en milieu bancaire*. Mémoire présenté pour l'obtention du graduat en comptabilité, Institut des Carrières Commerciales, Bruxelles.

Alter, S. (2002). The work system method for understanding information system and information system research. *Communications of the Association for Information Systems*, *9,* 90-104.

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

Alter, S., & Sherer, S. A. (2004). Information system risks and risk factors: are they mostly about information systems?. *Communications of the Association for Information Systems, 4*, 29-64.

Carvalho, J. A. (2000). Information System? Which one do you mean?. *Proceedings of the ISCO 4 Conference, Kluwer.Academic Publishers*. 259-280.

Ciorciari, M., & Blattner, P. (2008). Enterprise risk management maturity-level assessment tool. *The 6th ERM Symposium*.

Elmaallam, M., & Kriouile, A. (2011). Towards a model of maturity for IS risk management. *International Journal of Computer Science & Information Technology (IJCSIT)*, *3,* 171-188. http://dx.doi.org/10.5121/ijcsit.2011.3414

Goldstein, J., Benaroch, M., & Chernobal, A. (2008). IS-Related Operational Risk: An Exploratory Analysis. *In Proceedings of the 14th Americas Conference on Information Systems (Toronto, ON, Canada August 14th-17th, 2008),* 1-7.

IFACI, PriceWaterhouse-Coopers & Landwell. (Eds.).(2005). *Le management des risques de l'entreprise-cadre de référence - Techniques d'application - COSO II Report. 2005*. Edition Organisation.

IFACI. (Ed). (2009). *Introduction des normes*. p. 45.

ISO. (Ed). (2005). *Information technology - Security techniques - Code of practice for information security management*. Switzerland: ISO.

ISO. (Ed). (2008). *Information technology - Security techniques -Information security risk management*: Switzerland: ISO.

ISO. (Ed). (2009). *Management du risque Principes et lignes directrices*.

Mayer, J., & Fagundes, L. L. (2009). A model to assess the maturity level of the risk management. *Process in Information Security. 4rd IFIP/IEEE International Workshop on BDIM*. http://dx.doi.org/10.1109/INMW.2009.5195935