# TOWARDS A MODEL OF MATURITY FOR IS RISK MANAGEMENT

Mina ELMAALLAM[1] and Abdelaziz KRIOUILE[2]

[1] IMS Team, SIME Lab., ENSIAS, Rabat, MOROCCO
*elmaallam@gmail.com*
[2] IMS Team, SIME Lab., ENSIAS, Rabat, MOROCCO
*kriouile@ensias.ma*

***ABSTRACT***

*The risk management is an indispensable discipline for any organisation to acheive its objectives. As the IS (Information Systems) are key assets for organisations, managing IS risks becomes more and more important especially within a world in perpetual change. Since IS risk management creates plus value, it must follow a process of continuous improvement orchestrated by a model of maturity indicating in every time the runways of improvement. The studied literature shows the lack of a model that treat the maturity of the IS risk management and that consider all IS components. The present article has for purpose to initiate reflexion around this area and deliver a model of IS risk management maturity. First, we indicate IS definition that will fix the scope (All things concerned by IS risk management). Second, we define the IS risk management process that will fix the way (Activities used in IS risk manaegement). Third, we develop the maturity model for IS risk management. At the end, we conclude with perspectives opened to this work.*

***KEY-WORDS***

*Information system, Risk, Risk management, Model of maturity, Life cycle.*

## 1. INTRODUCTION

IS (Information Systems) are a key component for any organisation. Therefore, this asset needs to be protected against any threats. The best way is to establish an effective IS risk management process that fulfills a number of critera such as:

- The consideration of the company context during risks identification and classification,
- The informations relevance used for risks appreciation,
- The use of suited tools for risks formalizing and following-up,
- The Efficiency of the risks treatement plan,
- The staff awareness degree to the importance of risk management.

The efficiency measure of the risk management process can be made by the evaluation of these criteria compared to an internal company reference. But it will give a more real and more credible image if it is made by ensuring a risk management benchmarking related to companies operating in similar business sectors.

Benchmarking is very important. Indeed, it is a way to enrich the criteria and to identify ways to improve the process of risk management. Benchmarking can be done in different ways in which the best is to refer to a repository called maturity model [1].

We deduce then that each company that want to protect and develop a safe IS, must implement an effective risk management process, and submit it to a continuously evaluation by using an appropriate maturity model.

DOI : 10.5121/ijcsit.2011.3414 

The aim of this paper is to initiate a reflection on an IS risk management maturity model by analyzing two aspects. The first one is about the main axis to use to evaluate the maturity. The seconde one is about the main controls to use to measure every axis.

The analysis of the IS topic as well as the first IS researches, confirm the importance to answer an essential question before deepen our reflection: what défintion to adopt for an information system? Indeed, we found confusion in the literature between information systems (IS) and information technology (IT). Hence the confusion extends to the risk management and maturity assessment. The existing maturity models address the maturity of IT risk management and not IS risk management. The reflection initiated in this paper aimes to propose a maturity model for IS risk management after eliminating any ambiguity in the definition of IS.

The next section of this paper shows the IS definition that we will adopt throughout our reflection. This section presents also the descripion of the IS life cycle.

The third section treats the IS risk management. It presents the risks conceptualization and risk management process.

The fourth section presents the related works on maturity model for IS risk management.

The fifth section presents the proposed model for measuring the maturity of risk management taking into account the IS definition given in the second section.

In the sixth section, we conclude this paper and list the planned next works.

## 2. INFORMATION SYSTEMS: DEFINITION AND LIFE CYCLE

### 2.1. Definition of information systems

There are several definitions of an information system [2]. In our study, we adopted the definition of the IS as a work system [3]. 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 [3].

The components of a work system are:

**Infrastructure.** Infrastructure includes human, informational, and technical resources that the work system relies on even though these resources exist and are managed outside of it and are shared with other work systems. Infrastructure includes support and training staff, shared databases, and networks and programming technology [4].

**Strategies.** To the extent to which they are clearly articulated, the work system's strategy and the organization's strategy may help in explaining why the work system operates as it does. Examples of work system strategies include assembly line approach versus a case-manager approach and mass customization approach versus a commodity approach or a manually customized approach [4].

**Environment.** Environment includes the organizational, cultural, competitive, technical, and regulatory environment within which the work system operates. These factors affect system performance even though the system does not rely on them directly in order to operate. The organization's general norms of behavior are part of its culture, whereas more specific

behavioral norms and expectations about specific activities would typically be considered part of the business process [4].

**Technologies.** Technologies include tools (such as cell phones, projectors, spreadsheet software, and automobiles) and techniques (such as management by objectives, optimization, and remote tracking) that work system participants use while doing their work. Even when substantially computerized, specific tools (such as cars) and techniques (such as use of checklists) may or may not be associated with IT in a particular situation. Especially as adapted to fit a work system's peculiarities, technologies are viewed as integral parts of that work system and their affordances (such as a cell phone affording mobility) tend to be evident to system participants. In contrast, technical infrastructure includes technologies such as computer networks and programming technologies that are shared by other work systems and are often hidden or invisible to work system participants [4].

**Information.** Information includes codified and non-codified information used and created as participants perform their work. Either type of information may or may not be captured on a computer. The distinction between data and information is secondary when describing or analyzing a work system because data not related to the work system is not directly relevant [4].

**Participants.** People who perform at least some of the work in the business process are the work system participants. Some may use computers and IT extensively, whereas others may use little or no technology. Whether or not particular participants happen to be technology users, when analyzing a work system the more encompassing role of participant is more important than the more limited role of technology user [4].

**Business processes.** The work performed within the work system can be summarized in terms of one or more business processes whose steps may be defined tightly or may be relatively unstructured. Activities within each step include combinations of information processing, communication, sense making, decision making, thinking, and physical actions. As workplace researchers point out repeatedly, the actual operation of business processes often deviates from the idealized business processes that were originally designed or imagined. In addition, different participants may perform the same steps differently based on differences in skills, training, and incentives [4].

**Products & services.** Products and services are the combination of physical things, information, and services that the work system produces. They may include physical products, information products, services, intangibles such as enjoyment and peace of mind, and social products such as arrangements, agreements, and organizations. The terms products and services are used instead of "outputs" because that term brings too many mechanistic and computer-related connotations, especially when services and intangibles are involved [4].

**Customers.** People who receive direct benefit from products and services the work system produces include external customers who receive the organization's products and/or services and internal customers who are employees or contractors working inside the organization. According to the theory of Total Quality Management (TQM), a work system's customers are typically best able to evaluate its products and services. Customer satisfaction is often linked to the entire customer experience, starting from determining requirements and acquiring the products or services [4].

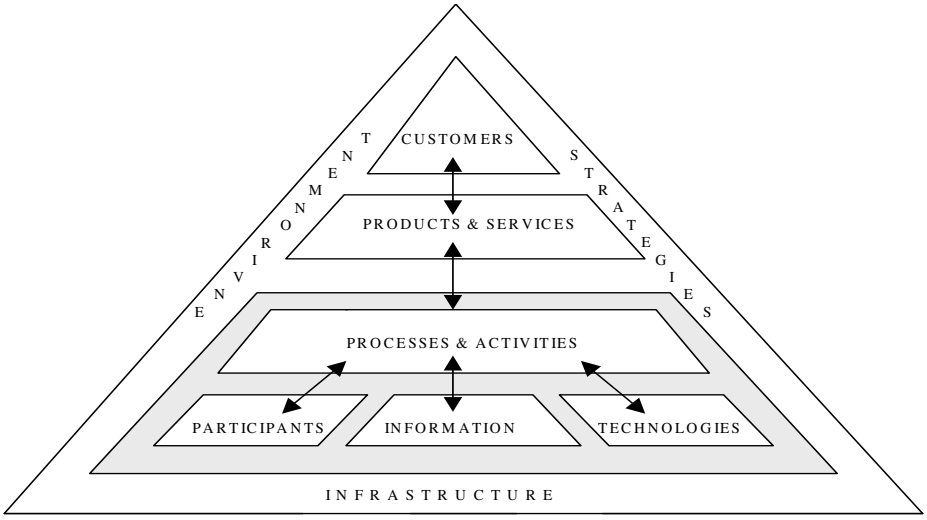


Figure 1. The Work System Framework [3]

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 [3].

To illustrate this IS definition, we give an example (Table.1) for a CRM IS (Customer Relationship Management) that handles a pension fund.

Table.1. Exemple of IS defined as Work System

| Component | Example |
|---|---|
| Infrastructure | - Customers reception space<br>- Call center<br>- Servers machines running applications software<br>- Telephony |
| Strategies | - Customers satisfaction is a strategic objective<br>- Availibality of 24/24 and 7/7<br>- Offering teleservices to the customers |
| Environement | - The process approach established<br>- To Satisfy the customers is a culture |
| Technologies | - CRM software<br>- Queue management software<br>- EDM (Electronic Document Management)<br>- Web sites |
| Information | - Paper-based information<br>- Computer-based information |
| Participants | - Responsible of customers<br>- Tele-Advisors<br>- IT Specialists<br>- Process owner |
| Business process | - Customers relationship<br>- Recovery<br>- Career management<br>- Payment |
| Products & services | - Update of the situation<br>- Consultation of the situation<br>- Certificate of pension |
| Customers | - Retired<br>- Employers |

### 2.2. IS Life cycle

Given the temporal nature of risk [5], management should take into consideration the evolution of the systems studied over time. This evolution is called life cycle. We adopted the life cycle WSLC (Work System Life Cycle) proposed for a work system [6]. This definition is in line with the definition adopted for the IS. The WSLC model is based on the following terminology [6]:

- Life cycle: the main lines of a typical road in the development of an entity type , as a working system, an information system, a project, or of a software [6],
- Iterations: a system life cycle is constituted by one or several iterations of four phases [6],
- Four phases: the initiation, the development, the implementation, the exploitation and maintenance [6]. The same phase decomposition is given in the definition of the software engineering life cyle [7].

## 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 [8].

For the company, as an economic unit, the risks are divided into five categories [9]:

- Market risk: results in exposure to fluctuations in market parameters such as interest rate risk, exchange rate risk [9].
- Credit risk: investor's risk of loss arising from a borrower who does not make payments as promised [9]
- Operational risk: represents threats that an organization faces in managing daily activities [9].
- Political, regulatory, and legal risks: those risks condition the immediate external environment of the company and set or change it competitive position [9].
- Liquidity risk: the risk of lack of funds at any time to meet the immediate payment of its commitments [9].

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 [10].

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 [11]:

**Components of the risks or types of negative results:** The first risks conceptualization identifies different types of negative outcomes [11]. (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 [11].

**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 [11].

### 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 [12].

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 [13] has five main activities (Figure 2):

**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 organisation defines the context according to 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 risk 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 [14].

**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 [13].

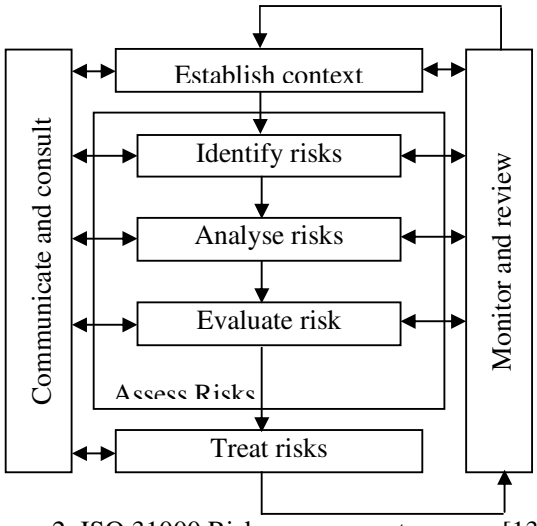


Figure 2: ISO 31000 Risk management process [13]

# 4. RELATED WORKS

In this chapter we present the existing in terms of maturity models for risk management in all various disciplines related to information systems.

## 4.1. Risk Maturity Model: RMM

The RMM model is the first risks maturity model. It was created by Hillson in 1997. It is the basis for many maturity models. This model measures the maturity of risks in four areas: Culture, Process, Experience and Application [15].

## 4.2. Risk Management Maturity Model: RMMM

This model was developed in 2002 by INCOSE, a small business working team in the field of project risk management [16]. It is a simplified maturity model, based on the RMM, and conceived to target as quickly as possible all weaknesses. It is applicable to all types of organisation and projects accross all sectors [16].

The RMMM proposes four levels of maturity: level 1: ad hoc, Level 2: initial, Level 3: repetitive and Level 4: managed, and it is centred on four domains: culture, Process, Experience and Application [15].

## 4.3. Risk management maturity model in IS security: MMGRSeg

This model was created to evaluate the level of risk management process maturity in the field of the information security [17].

This model is aligned on the ISO/IEC 27005 standard. It is based on [17]:

- Three stages: maturity, Immaturity and Excellence,
- Five levels of maturity,
- Forty three objectives of control,
- A map of control,
- A tool for assessing the maturity level of the risk management process activities,
- RACI matrix relative to each risk management process activity,
- A dashboard of the risks.

## 4.4. Maturity Model of RISK IT Framework

RISK IT defines three risk domains: risk governance, risk evaluation and risk response. Each domain has a maturity model high level and a detailed maturity model.

The high level provides six levels from 0 to 5 [18]:

- 0: Non existent,
- 1: Initial/Ad Hoc,
- 2: Repeatbale but intuitive,
- 3: Defined process,
- 4: Managed and measurable,
- 5: optimised.

The detailed models are built around the following attributes [18]:

- Raising sensitization and communication,

- Responsibilities and imputability,
- Definition of the objectives and the associated measures,
- Politics, standards and procedures,
- Skills and expertises,
- Tools and automation.

### 4.5. Capability Maturity Model Integration (CMMI)

The CMMI is a model conceived by the Software Engineering Institute (SEI) to favor the improvement of organizations processes and their capacity to manage, to develop and to maintain their products/software. CMMI has two representations: staged and continue. The permanent representation has six levels of capacity, numbered from 0 to 5, whereas the representation stage contains five levels of maturity: initial, managed, defined, quantitatively managed and optimizing [19].

### 4.6. COBIT

COBIT provides a framework for the control and governance of IT-based solutions and services. It decomposes any IT system into thirty four processes related to four functional domains [20]:

- Plan and organise (PO - 10 processes),
- Acquire and implement (7 processes),
- Deliver and support (13 processes),
- Monitor and evaluate (4 processes).

These four domains cover 318 objectives of control. The IT risk management is assured by the process PO09 which is decomposed into six activities from PO9.1 to PO9.6. Each activity covers a specific control objective [21].

### 4.7. OPM3

OPM3 is a model developed by the Project Management Institute (PMI). It is based on Project Management Body of Knowledge (PMBOK) [22]. It includes three domains: project, program and portfolio, which refer to four levels of maturity: standardization, measure, control and continuous improvement [23].

The Table 2 gives a summary of discussed models in this section.

Table 2. Summary of IS risk management maturity models

| Model | Model description (domains, levels) | IS Specification |
|---|---|---|
| RMM | - Domains: Process , experience, culture, application<br>- Maturity level: 4 levels | Treats the maturity of the risk management in a general way. No specificity for IS |
| RMMM | - Domains : risk management process activities<br>- Maturity level: 5 levels. | Can be used partially to the management of IS projects |

| | | |
|---|---|---|
| MMGRSeg | - Domains : risk management process activities<br>- Maturity level: 5 levels | Concerns a part of IS: the information security |
| RISK IT | - Domains: risk governance, risk assesment, risk response<br>- Maturity level: 5 levels | Concerns the maturity of IT risk management |
| CMMI | - Domains: process management, project management, software engineering<br>- Maturity level: 5 levels | Concerns only software development |
| COBIT | - Domains: IT plan and organise, IT acquire and implement, IT deliver and support, IT monitor and evaluate<br>- Maturity level: 5 levels | Concerns IT governance |
| OPM3 | - Domains: project, program and portfolio<br>- Maturity level: 4 levels | Can be used partially to the management of IS projects |

As indicated in the Table 2, the existing models define the control objectives only for a part of an IS as information security (MMGRSeg) or a corresponding discipline such as the IT governance (COBIT, RISK IT) or the IS project management (OPM3). No model treats the IS risk maturity by considering all IS components.

## 5. A PROPOSED MODEL OF MATURITY FOR ASSESSING THE IS RISK MANAGEMENT

### 5.1. 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:

- 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:

- List all the IS,
- For each IS:
  - 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 activitities.
- 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 3.

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.

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.

Table.3. Illustration of IS Risk Management Matutity 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** |

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:

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

## 5.2. 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 [24]. 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:** Normalised**:** 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**: Optimised: Risk management activities are part of a continuous improvement process based on the results and measurements of the level 4.

## 5.3. 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 [25]. The table 4 gives the list that we propose for control elements. Thoses control elements are defined through a study of risk factors [11] related to each IS constituent.

Table 4 Description of the control elements for the IS constituents

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

## 5.4. 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 organisation will be reached and that the unwanted events will be avoided or deleted and corrected [26].

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.

### 5.4.1. 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.

### 5.4.2. Objectives of control of the activity “Risk assesment”

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.

### 5.4.3. Objectives of control of the activity "Risk treatement"

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.

### 5.4.4. 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.

### 5.4.5. 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.

## 5.5. Measure of the maturity

### 5.5.1. 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 echelle of measure. The table 5 gives an example of evaluation question.

Table.5. exemple of evaluation question

| Composant | Control element | Activity | Control objective | Example |
|---|---|---|---|---|
| Participants | Skill and expertise | Establishment of the context | EC.1. Develop an identification sheet of IS studied | Is there a repository of expertise? |
| Participants | Communication | Risk assesment | AP.4. Apply the methodology of appreciation of the risks defined in the context | Is there a checklist to verify the spread of information? |

### 5.5.2. 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 maximlal 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 6 presents the control map for the various components:

Table 6 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 Assesment | No control is implemented | AP.1, AP.2, AP.3 | AP.4 | AP.5, AP.6 | AP.7, AP8 |
| Risk treatement | 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 |

## 6. CONCLUSION

Information systems are an important tool for business development. Thus, IS risk management is crucial and indispensable activity in any organisation. However, this management should be evaluated continuously to ensure its efficiency and create value for which it exists. This is done through a maturity model of IS risk management.

The proposed model aims to assess the maturity of IS risk management within a company. It is interested in IS defined as a work system and therefore including all its constituents (infrastructure, strategy, environment, participants, processes, products/services and customers) in contrast to existing models that are limited to some IS fields such as information security (MMGRSeg), software development (CMMI) and IT governance (COBIT & RISK IT).

The proposed model is based on the IS life cycle, IS constituents and its control elements, IS risk management process and control objectives of its activities, and finally the control map that defines the maturity levels.

This paper presented the first track by considering one IS and deactivating the impact of IS life cycle. In perspective, we envisage in a next work to:

- Consider the IS life cycle phases and update the control elements as well as the control objectives,
- Consider all the company IS and consolidate its maturity level,
- Apply this maturity model on a real case study in order to verify its applicability and efficiency. Then, adjust the maturity model depending on the case study results.

## REFERENCES


- [1] N.Nayab, (2010),''Characteristics of Good Project Risk Management'', Bright Hub, Oct 12, 2010, http://www.brighthub.com/members/nayab.aspx
- [2] João Álvaro Carvalho,(2000) ''Information System? Which One Do You Mean? '', Proceedings of the ISCO 4 Conference, Leiden, Holanda, 20 -22 September 1999, Kluwer.Academic Publishers, 2000, pp.259-280
- [3] Steven Alter, (2008), '' Defining information systems as work systems : implications for the IS field '', European Journal of Information Systems (2008) 17, pp448–469
- [4] Steven Alter, (2002), " The Work System method for understanding Information System and Information System research", Communications of the Association for Information Systems (Volume 9, 2002) pp 90-104
- [5] Steven Alter & Susan A. Sherer, (2004), '' A general, but readily adaptable model of information system risk '', Communications of the Association for Information Systems (Volume14, 2004) pp1-28
- [6] Steven Alter, (2001), '' Which life cycle - - - work system, information system, or software? '', Communications of AIS Volume 7, Article 17, pp1-54
- [7] F.Villeneuve & Y. Soler , (2001), '' Présentation du cycle de vie d'un système d'information'', CNRS, pp1-6
- [8] IFACI, (2009), Institut Français de l'Audit et Contrôle Interne, Introduction des normes, April 2009, p 45

- [9] Agnaou Akim, (2007-2008), ''La gestion du risque opérationnel, application à la lutte contre la fraide en milieu bancaire ''. Mémoire présenté pour l'obtention du graduat en comptabilité. pp 8-9.
- [10] James Goldstein & Michael Benaroch & Anna Chernobal, (2008), "IS-Related Operational Risk: An Exploratory Analysis ", AMCIS 2008 Proceedings, Proceedings of the Fourteenth Americas Conference on Information Systems, Toronto, ON, Canada August 14th-17th, paper 89, pp1-7
- [11] Lee Steven Alter & Susan A. Sherer, (2004), '' Information system risks and risk factors: are they mostly about information systems? '', Communications of the Association for Information Systems (Volume14, 2004) pp29-64
- [12] IFACI, PriceWaterhouse-Coopers, Landwell, (2005),''Le management des risques de l'entreprise Cadre de référence - Techniques d'application - COSO II Report'' , Edition Organisation, p.5
- [13] ISO ,(2009), ISO, groupe de travail du bureau de gestion technique de l'ISO, Management du risque Principes et lignes directrices, Numéro de référence ISO/FDIS 31000:2009(F)
- [14] ISO , (2008), "Information technology - Security techniques –Information security risk management: ISO/IEC 27005:2008", Switzerland: ISO,
- [15] BEGÜM ÖNGEL, (2009), "Assessing risk management maturity: a framework for the construction companies", A thesis submitted to the graduate school of natural and applied sciences of middle east technical university,
- [16] INCOSE ,(2002), Formal Collaboration: INCOSE Risk Management Working Group; Project Management Institute Risk Management Specific Interest Group; UK Association For Project Management Risk Specific Interest Group, Risk Management Maturity Level Development
- [17] Janice Mayer & Leonardo Lemes Fagundes,(2009), "A Model to Assess the Maturity Level of the Risk Management Process in Information Security", 4rd IFIP/IEEE International Workshop on BDIM
- [18] ISACA , (2010) RISK IT Framework, ISACA
- [19] M. B. Chrissis & M. Konrad & S. Shrum, (2005), "CMMI® - Guidelines for Process Integration and Product Improvement", United States: SEI
- [20] Eric LELEU, (2009), Le COBIT : L'état de l'Art, Socle de la gouvernance des SI, CNAM 2008 / 2009, GLG102 – Techniques et normes pour la qualite du logiciel
- [21] Dominique MOISAND & Fabrice GARNIER DE LABAREYRE & Didier Lambert & J.-M. Chabbal & T. Gasiorowski & F. Legger & L. Vakil, (2009), COBIT pour une meilleure gouvernance des systèmes d'information, Groupe Eyrolles,
- [22] PMI , "A guide to the project management body of knowledge(PMBOK Guide)", Upper Darby, PA, 2000.
- [23] PMI , (2008), Project Management Institute (PMI), "PMI Fact Sheet", USA: PMI, 2006, available in: <http://www.pmi.org>, access in: 10 May 2008.
- [24] Janice Mayer & Leonardo Lemes Fagundes, (2009) " A Model to Assess the Maturity Level of the Risk Management Process in Information Security", 2009 IFIP/IEEE Intl. Symposium on Integrated Network Management — Workshops, pp61-70
- [25] Maria Ciorciari & Dr. Peter Blattner, (2008), " Enterprise Risk Management maturity-level assessment tool", ERM Symposium April 14-16, 2008 Chicago
- [26] ISO , (2005), "Information technology - Security techniques - Code of practice for information security management: ISO/IEC 27002:2005", Switzerland: ISO, 2005.

**Authors**

**Mina ELMAALLAM:**

- ✓ Computer science engineer from ENSIAS
- ✓ Project Manager, Risk Manager
- ✓ PhD student (ENSIAS-Rabat)

**Abdelaziz KRIOUILE:**

- ✓ Professor of the Higher education (ENSIAS-Rabat)
- ✓ Doctorate of State in sciences of the University Mohammed V Rabat, on 1995