Journal of Computer Science

Original Research Paper

Optimizing the Deployment of the Overall Maturity Improvement Plan for Information Systems Risk Management

[1]Fatima Ezzahra Ettahiri, [2,1]Mina El Maallam, [3]Hicham Bensaid and [1]Mahmoud Nassar

[1]*IMS Team, ADMIR Laboratory, ENSIAS, Mohammed V University, Rabat, Morocco*
[2]*IRIS Team, MIKS Laboratory, ESI, Rabat, Morocco*
[3]*Laboratory of Mathematics, Computing and Applications, National Institute of Posts and Telecommunications, Morocco*

Article history
Received: 12-07-2021
Revised: 19-02-2022
Accepted: 12-01-2022

Corresponding Author:
Fatima Ezzahra Ettahiri
IMS Team, ADMIR
Laboratory, ENSIAS,
Mohammed V University,
Rabat, Morocco
Email: fatimaezzahraettahiri@gmail.com

Abstract: Maturity models contribute considerably to the continuous improvement of the various business processes. However, the most important challenge for these tools after assessing maturity is how to define effective and efficient improvement plans especially in the case of an organization having multiple Information Systems (IS). This study presents an algorithm for optimizing the deployment of the overall maturity improvement plan for risk management of information systems. The purpose is to help decision makers identify which actions should be accomplished for each information system, with optimizing efforts needed to reach the global maturity level fixed by the top-down improvement strategy. The application of the proposed algorithm made it possible to define the improvement actions to be undertaken by a company in an optimized way for each of its IS to reach an overall target maturity. The calculation of the number of steps to be taken through the maturity matrix shows the effort gained. That gain can be the human and financial cost for the completion of the various necessary tasks to implement the objectives of control.

Keywords: Maturity Model, Maturity Improvement, Information System, Risk Management, Optimization

Introduction

Information systems governance is nowadays critical for companies' management success and effectiveness. As introduced in (Elmaallam and Kriouile, 2012), the information system governance is the identification and achievement of the required action plans and means, to reach its objectives. Risk management is one of its main pillars.

Based on the generic definition proposed by (ISO, 2009-a), information system risk management is all activities coordinated with the aim of managing and piloting IS against risk. The latter is "the effect of uncertainty on objectives" (ISO, 2009a).

In the Internet age, information systems face rapid and unpredictable changes; the frequency of attacks and abuses is not constant, it varies along with time and skills of users and hackers, hence the importance of protecting the information system from attacks and abuses and suggesting countermeasures that allows IS to protect itself in an efficient way and with minimal costs (Arogundade *et al*., 2020). In addition, organizations are nowadays carrying out their activities within complex economic and environmental circumstances which make implementing risk monitoring strategies imperative, because of the intrinsic link between risks and business activities as stated in (Settembre-Blundo *et al*., 2021).

Information system risk management is consequently a vital activity in the life of the company. Indeed, it helps managers to make the right decisions, protects the company against threats causing different types of losses and contributes to the optimal allocation of resources. (Salvati, 2008).

The benefits of IS risk management, as mentioned, make this discipline not only a necessity for IS governance but also a key factor for its success. Therefore, the evaluation and improvement of this activity has become a necessity. This improvement should be done according to a well-defined framework ensuring cost control of its implementation and ensuring its continuity. Hence the interest of maturity models to assess the level of maturity of this discipline within companies and conclude the necessary actions for its improvement.

In a previous work, we proposed a design process (Elmaallam and Kriouile, 2014a). Using this process, we have implemented a maturity model devoted to IS risk management. Subsequently, we were interested in the definition of treatment plans by proposing an algorithm to list all the actions required to attain a desired maturity level for a single information system (Amraoui *et al*., 2019). Nevertheless, the latter is only useful when the adopted improvement strategy is a Bottom- up type. In the present work, we are interested in a Top-down strategy. To the best of our knowledge, we are not aware of any existing work tackling this aspect. We know no algorithm proposing, given a risk management maturity level for a global information system, the required risk management maturity level for each information system while optimizing required effort.

Background

Risk Management Process for Information Systems

According to (Alter, 2008) 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 internal or external customers. In spite of the multitude of IS definitions (Carvalho, 2000), this one is the most complete for our research context.

Risk management aims to identify, analyze, assess risks and then select the best strategy and more effective actions to deal with them. This process should consider the risk appetite defined by the enterprise. The methods and processes devoted to IS risk treat only some aspects like security or IS project management. Therefore, we adopt the ISO 31000 process (ISO, 2009-b) since it is generic and consistent with our research topic.

According to ISO 31000, the risk management process defines five principal activities (ISO, 2009-b):

- Scope, Context, Criteria in which the process context is defined
- Risk assessment in which the risks are identified, analyzed and evaluated
- Risk treatment in which the strategies and actions to deal with risk are defined
- Communication and consultation to make all stakeholders involved and informed during the process
- Monitoring and review to ensure that the risk management principles are followed and consider any changes that can impact the process
- Recording and reporting all the important facts and results of the process

Maturity Model Architectures

Maturity models contribute to the self-assessment of the company. They also offer the latter a benchmark against its competitors and help it to improve according to its strategy, its objectives and its means. Professionals as well as researchers are increasingly interested in these models (Poeppelbuss *et al*., 2011).

Maturity models are usually represented as levels or stages (Röglinger *et al*., 2012). These levels give the state of maturity of the company in relation to a given activity (Rosemann and de Bruin, 2005). The maturity models should also guide the company in defining its maturity improvement plan (Iversen *et al*., 1999).

The literature defines three types of architecture representing maturity models. The first two are called “fixed level architectures” and are: The staged and the continuous architectures. One of the typical examples of a fixed-level model is the CMMI. The third architecture is called "Focus Area architecture" (FA) (Koomen and Pol, 1999). Next section details the latter given its accordance with our research context.

Focus Area Model

The FA architecture is based on two principles: Each domain in the FA model can have its own improvement and the interdependence between domains is considered.

Table 1 illustrates this architecture. The enterprise has level 2. But each area or domain has its own level. The area 1 has level m. the area 2 has level 2. Etc.

“Focus Area (FA)” (Steenbergen *et al*., 2010) is a maturity model design approach developed using the DSR (Design Science Research) process (Peffers et al., 2008). FA Maturity models aim to support the continuous and progressive improvement of software testing (Koomen and Baarda, 2006).

The design of a maturity model based on the FA architecture gives rise to a maturity matrix (Elmaallam *et al*., 2019). Figure 1 gives an example. This latter contains 6 areas and 8 levels. The letters A, B, C, D and E are the required objectives of control for each level.

In this example, an enterprise reaches an overall maturity level '2' (column with header 2) if:

- All capacities located in the column corresponding to the level '2' are verified
- All capacities located in the left of the column corresponding to the level '2’ (columns 0 and 1) are verified
- There is at least one capacity on the right of the column corresponding to the level '2' that is unverified

The Isr3m Model for Assessing the Information Systems Risk Management Maturity

In this section, we present the model used for the application of our algorithm which will be defined in the next section: The "Information Systems Risk Management Maturity Model (ISR3M)" (Elmaallam *et al*., 2019). The objective of the latter is assessing the maturity of IS risk management. This model defines an information system as particular case of a work system (Alter and Sherer, 2004) and uses the ISO 31000 framework and the generic management cycle (Sienou, 2009) for the risk management process (Elmaallam *et al*., 2019). The architecture adopted is FA architecture (Elmaallam *et al*., 2019).

Figure 2 presents the ISR3M maturity matrix. The model proposes 12 maturity levels and 18 areas (Elmaallam *et al*., 2019):

- RM (Risk Management) Principles (PRM)
- Mandate and commitment (ME)
- Framework design (CCO)
- Risk management implementation (MOE)
- Monitoring and reviews (SRC)
- Continual improvement (ACC)
- External context (ECX)
- Internal context (ECI)
- Process context (ECP)
- Risk management criteria (ECC)
- Risk identification (API)
- Risk analysis (APA)
- Risk evaluation (APV)
- Selection of treatment option (TSO). - Elaboration of Treatment Plan (TEP)
- Implementing of treatment plan (TMP)
- Process monitoring and review (SR)
- Recording (Eng)

Figure 3 presents an example of an assessment (in blue) of the maturity of a risk management information system, while Fig. 4 gives the control objectives (in green) to be achieved after the improvement process.

Each organization has a set of different information systems which have different goals, importance and contribution (weight) in strategic objectives. The global risk management maturity of an information system is the consolidation of its information systems risk management maturities. This consolidation is given by one of the three calculation methods: The weighted average (according to each IS weight), the maximum IS maturities values and the minimum IS maturities values. To improve the IS risk management maturity, the organization can opt for one of two approaches: Bottom- up or Top-down.

In the first approach, we define for each IS the target maturity levels and then the control objectives required to reach them (Amraoui *et al*., 2019). Improving the overall maturity results from improving the maturities of each information system and aggregating the local achievements into global one.

The other approach consists in defining the target maturity level as coded in the global maturity matrix and then dividing it into the local maturity matrix of each information system.

To solve this issue, we propose the algorithm described in Table 3.

We focus on this second approach. The problem is to define for each target control objective which control objective we have to improve and in which level taking into consideration the dependence of CO and the minimization of the improvement effort. To the best of our knowledge, no existing work addresses this issue.

Optimized Deployment of the Global Improvement Plan

The aim of this section is to present the "Optimized-declination-improvement" algorithm. This latest defines for each information system the control objectives to reach, starting from global target control objectives while minimizing improvement efforts.

To explain the algorithm, we provide an example on the area called "APA risk analysis" for nine information systems (from IS 1 to IS 9). The control objectives (for APA area) reached by those information systems are given in Table 2.

By "Global", we mean measure consolidation of the different information systems. In this case, this measure is the weighted average of the nine information systems capabilities (levels corresponding to the control objectives) for this area. An information system weight is calculated using its proportion of charge, cost and contribution in strategic objectives of the organization. The obtained global capability is APA.A which means that the risk analysis is done in terms of causes, consequences and probabilities but the analysis method is not formalized.

Table 1: Focus Area architecture

	Level 1	Level 2	…	Level m	…
Area 1	X	X	X	X	
Area2	X				
Area 3		X		X	X
…	X	X	X		
Area k		X	X		X

Table 2: Example of an initial configuration of an IS to be improved

IS 1	IS 2	IS 3	IS 4	IS 5	IS 6	IS 7	IS 8	IS 9	Global
APA .B	APA .A	APA .A	APA .A	APA .A	APA .A	APA .A	APA .A	APA .A	APA. A.

Table 3: The « Optimized-declination-improvement » algorithm.

Algorithm: « Optimized-declination-improvement »

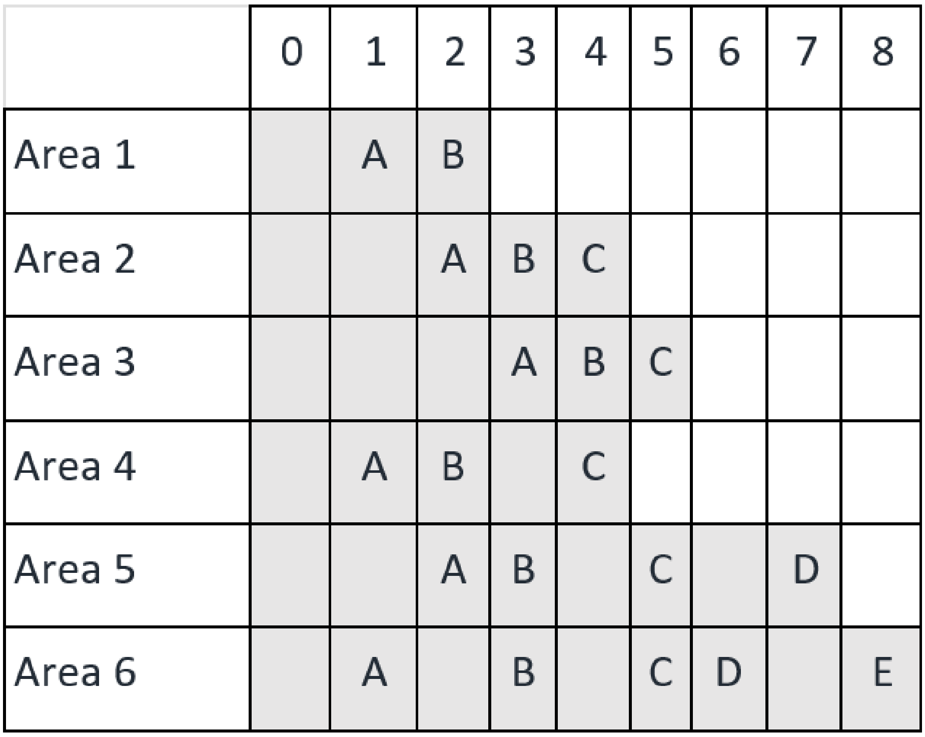
Purpose: To define control targets per information system from a global control target while optimizing improvement efforts.

We consider the following problem: Given a global control target of a set of information systems, we aim to define for each element in the set a control target such that the weighted sum of control targets of the elements in the set is greater than or equal the global control target of the set under the constraint that the improvement effort should be minimal.

The problem can be modeled as:

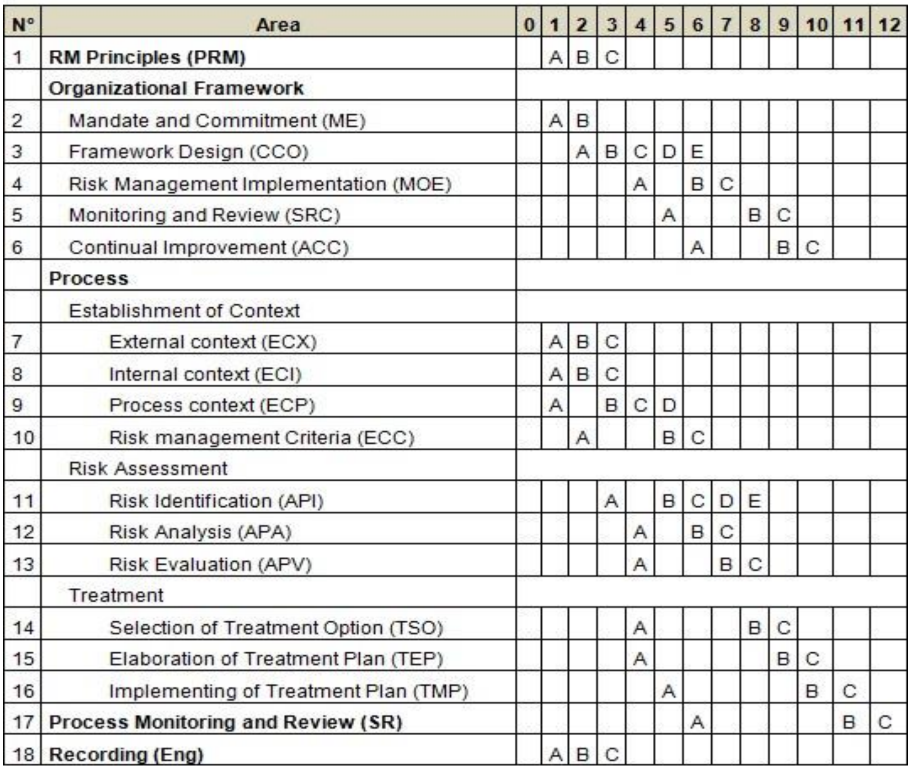
- Minimize the (linear) value: $z = (a_1 \times x_1) + (a_2 \times x_2) + \cdots + (a_n \times x_n)$ where:
    - n is the number of considered information systems
    - z represents the needed effort to reach the targeted improvement
    - For each Information System $IS_{i,}$ x_i is an integer representing the gap between the current value of the control target and the target value.
    - a_i is a weight representing additional efforts in terms of duty and cost for realizing the step x_i for the information system IS_i
- Under the (linear) constraints:
    - $(p_1.\,(n_{co1} + x_1)) + (p_2.\,(n_{co2} + x_2)) + \cdots + (p_n.\,(n_{con} + x_n)) \geq v$
    - For each i, p_i is the weight of the information system $IS_{i,}$ n_{oci} is the CO_i rank in the maturity matrix
    - For each i, $v_i \leq (n_{co} + x_i) \leq v^{max}{}_i$, where v_i is the current maturity level of IS_i and i
    - $v_i^{\max}$ the maximum level that can be reached by the control target n_{co} (control targets belong to well defined closed ranges)
    - v is the global target control objective.

This is a linear minimization problem under linear constraints to resolve.



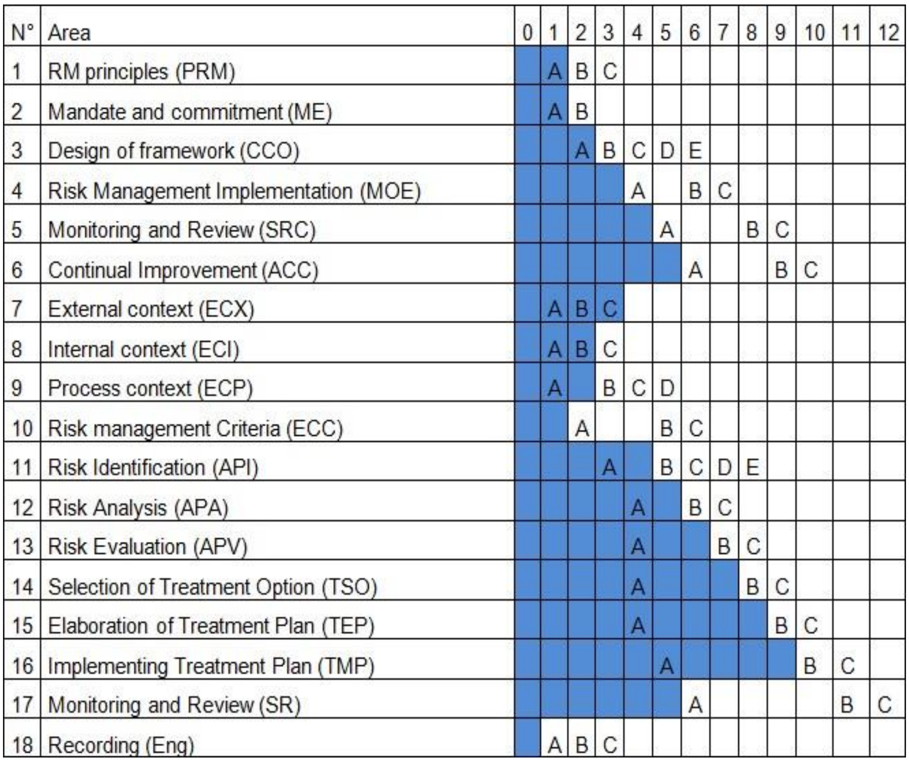
	0	1	2	3	4	5	6	7	8
Area 1		A	B						
Area 2			A	B	C				
Area 3				A	B	C			
Area 4		A	B		C				
Area 5			A	B		C		D	
Area 6		A		B		C	D		E

Fig. 1: Example of FA model maturity matrix



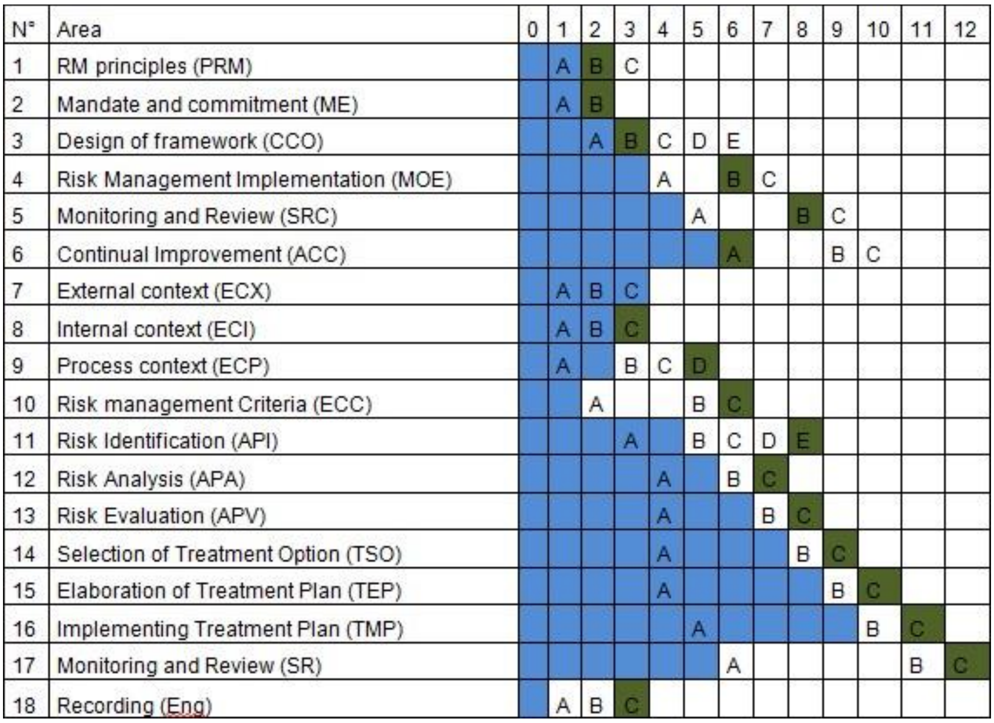
N°	Area	0	1	2	3	4	5	6	7	8	9	10	11	12
1	**RM Principles (PRM)**		A	B	C									
	Organizational Framework													
2	Mandate and Commitment (ME)		A	B										
3	Framework Design (CCO)			A	B	C	D	E						
4	Risk Management Implementation (MOE)					A		B	C					
5	Monitoring and Review (SRC)						A			B	C			
6	Continual Improvement (ACC)							A			B	C		
	Process													
	Establishment of Context													
7	External context (ECX)		A	B	C									
8	Internal context (ECI)		A	B	C									
9	Process context (ECP)		A		B	C	D							
10	Risk management 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 Option (TSO)					A				B	C			
15	Elaboration of Treatment Plan (TEP)					A					B	C		
16	Implementing of Treatment Plan (TMP)						A					B	C	
17	**Process Monitoring and Review (SR)**							A					B	C
18	**Recording (Eng)**		A	B	C									

Fig. 2: ISR3M maturity matrix (Elmaallam & Bensaid & Kriouile, 2019)



N°	Area	0	1	2	3	4	5	6	7	8	9	10	11	12
1	RM principles (PRM)	▨	▨ A	B	C									
2	Mandate and commitment (ME)	▨	▨ A	B										
3	Design of framework (CCO)	▨	▨	▨ A	B	C	D	E						
4	Risk Management Implementation (MOE)	▨	▨	▨	▨	A		B	C					
5	Monitoring and Review (SRC)	▨	▨	▨	▨	▨	A			B	C			
6	Continual Improvement (ACC)	▨	▨	▨	▨	▨	▨	A			B	C		
7	External context (ECX)	▨	▨ A	▨ B	▨ C									
8	Internal context (ECI)	▨	▨ A	▨ B	C									
9	Process context (ECP)	▨	▨ A		B	C	D							
10	Risk management Criteria (ECC)	▨	▨	A			B	C						
11	Risk Identification (API)	▨	▨	▨	▨ A	▨	B	C	D	E				
12	Risk Analysis (APA)	▨	▨	▨	▨	▨ A	▨	B	C					
13	Risk Evaluation (APV)	▨	▨	▨	▨	▨ A	▨	▨	B	C				
14	Selection of Treatment Option (TSO)	▨	▨	▨	▨	▨ A	▨	▨	▨	B	C			
15	Elaboration of Treatment Plan (TEP)	▨	▨	▨	▨	▨ A	▨	▨	▨	▨	B	C		
16	Implementing Treatment Plan (TMP)	▨	▨	▨	▨	▨	▨ A	▨	▨	▨	▨	B	C	
17	Monitoring and Review (SR)	▨	▨	▨	▨	▨	▨	A					B	C
18	Recording (Eng)	▨	A	B	C									

Fig. 3: ISR3M maturity matrix: example for an initial configuration (Elmaallam & Bensaid & Kriouile, 2019)



N°	Area	0	1	2	3	4	5	6	7	8	9	10	11	12
1	RM principles (PRM)	🟦	A	B	C									
2	Mandate and commitment (ME)	🟦	A	B										
3	Design of framework (CCO)	🟦	🟦	A	B	C	D	E						
4	Risk Management Implementation (MOE)	🟦	🟦	🟦	🟦	A		B	C					
5	Monitoring and Review (SRC)	🟦	🟦	🟦	🟦	🟦	A			B	C			
6	Continual Improvement (ACC)	🟦	🟦	🟦	🟦	🟦	🟦	A			B	C		
7	External context (ECX)	🟦	A	B	C									
8	Internal context (ECI)	🟦	A	B	C									
9	Process context (ECP)	🟦	A		B	C	D							
10	Risk management Criteria (ECC)	🟦	🟦	A			B	C						
11	Risk Identification (API)	🟦	🟦	🟦	A	🟦	B	C	D	E				
12	Risk Analysis (APA)	🟦	🟦	🟦	🟦	A	🟦	B	C					
13	Risk Evaluation (APV)	🟦	🟦	🟦	🟦	A	🟦	🟦	B	C				
14	Selection of Treatment Option (TSO)	🟦	🟦	🟦	🟦	A	🟦	🟦	🟦	B	C			
15	Elaboration of Treatment Plan (TEP)	🟦	🟦	🟦	🟦	A	🟦	🟦	🟦	🟦	B	C		
16	Implementing Treatment Plan (TMP)	🟦	🟦	🟦	🟦	🟦	A	🟦	🟦	🟦	🟦	B	C	
17	Monitoring and Review (SR)	🟦	🟦	🟦	🟦	🟦	🟦	A					B	C
18	Recording (Eng)	🟦	A	B	C									

Fig. 4: ISR3M Maturity matrix: Example for a target configuration (Elmaallam *et al*., 2019)

In the context of a "Top-Down" improvement strategy, we aim to improve the global maturity level of the APA domain from APA.A to APA.B mainly to reach a level of maturity where the organization can:

- Use tools and techniques for risk analysis
- Be able to obtain analytical results to assess the risks
- Make sure to contribute to the choice of treatment strategies and methods during the analysis
- Consider and communicate to the stakeholders, the degrees of confidence in the determination of the level of risk and its sensitivity to preconditions and assumptions
- Mention and highlight factors such as: The difference in opinion between experts, the uncertainty, the availability, the quality, the quantity and the validity of the relevance of the information, while optimizing the improvement of each information system

The problem is how to reach this global maturity level through the improvement of each information system maturity for this area, while minimizing the needed effort.

Application

The studied organization is a Moroccan public establishment. It has more than 300 employees. It attaches a great importance to IS and considers it as its biggest competitive advantage. IS risk management has been implemented within this organization for almost four years. It concerns both operational risk management and IS security risks. An IS urbanization mission gives the description of the studied IS in Table 4. The latest lists for each information system the nouns, the activities, the proportion of the global charge and cost, the contribution in the strategic objectives SO.1, SO2, SO.3 and SO.4 (1 for Weak contribution (W), 2 for Medium contribution (M) and 3 for High contribution (H)).

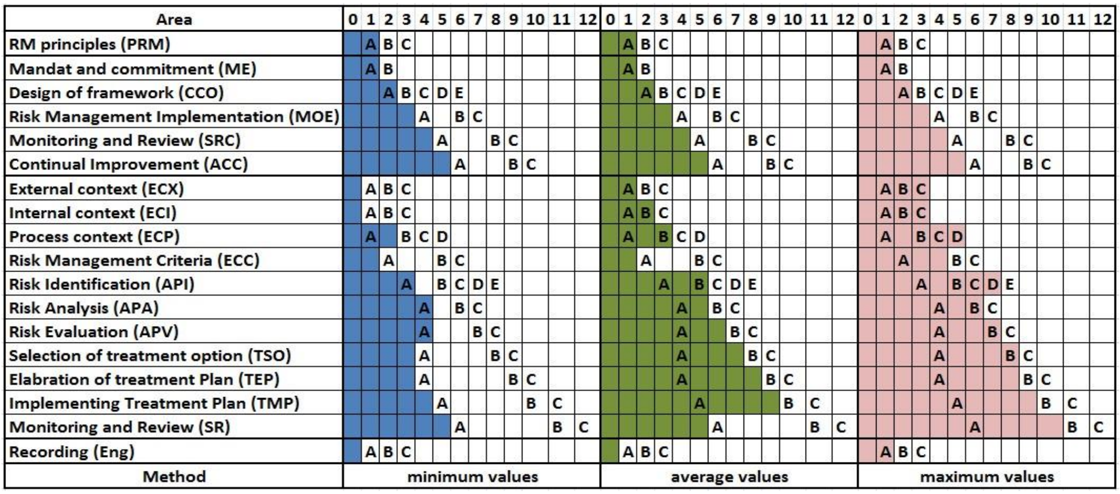
Figure 5 presents the overall result of the consolidated evaluations of the different information systems according to the three calculation methods: Weighted average (according to each IS weight), maximum values and minimum values of the studied information systems.

Following the analysis, the improvement strategy adopted by the evaluation team is the "Top-Down" approach with an improvement "by control objectives". The targets are defined through the "average values" of the previously defined control objectives with an improvement in some areas. This planned improvement is described in Table 5 through the target control objectives. The area PRM, ME, CCO, MOE, SRC and ACC are not concerned by this improvement. They maintain the same maturity levels.

We apply the improvement algorithm consisting in defining the targets by SI by optimizing the efforts and then defining for each IS the prerequisites for reaching these targets. It should be noted that the efforts made to achieve a CO_i control objective is in our case study the same for all information systems ($a_i = 1$).

The results using the matrix levels are given in Table 6 (the symbol "T" for "target" and "I" for "Initial"). The latter describes for each IS the values of the target levels corresponding to the target control objectives required to achieve the global target control objective with effort minimization.

According to the results presented above in Table 6 and the ISR3M matrix (Fig. 2), Table 7 gives the target control objectives for each information system.



Area	0	1	2	3	4	5	6	7	8	9	10	11	12
RM principles (PRM)	■	A	B	C									
Mandat and commitment (ME)	■	A	B										
Design of framework (CCO)	■	■	A	B	C	D	E						
Risk Management Implementation (MOE)	■	■	■	■	A		B	C					
Monitoring and Review (SRC)	■	■	■	■	■	A			B	C			
Continual Improvement (ACC)	■	■	■	■	■	■	A			B	C		
External context (ECX)	■	A	B	C									
Internal context (ECI)	■	A	B	C									
Process context (ECP)	■	A	■	B	C	D							
Risk Management Criteria (ECC)	■	■	A			B	C						
Risk Identification (API)	■	■	■	A		B	C	D	E				
Risk Analysis (APA)	■	■	■	■	A		B	C					
Risk Evaluation (APV)	■	■	■	■	A			B	C				
Selection of treatment option (TSO)	■	■	■	■	A				B	C			
Elabration of treatment Plan (TEP)	■	■	■	■	A					B	C		
Implementing Treatment Plan (TMP)	■	■	■	■	■	A					B	C	
Monitoring and Review (SR)	■	■	■	■	■	■	A					B	C
Recording (Eng)	■	A	B	C									
Method	minimum values												

Area	0	1	2	3	4	5	6	7	8	9	10	11	12
RM principles (PRM)	■	A	B	C									
Mandat and commitment (ME)	■	A	B										
Design of framework (CCO)	■	■	A	B	C	D	E						
Risk Management Implementation (MOE)	■	■	■	■	A		B	C					
Monitoring and Review (SRC)	■	■	■	■	■	A			B	C			
Continual Improvement (ACC)	■	■	■	■	■	■	A			B	C		
External context (ECX)	■	A	B	C									
Internal context (ECI)	■	A	B	C									
Process context (ECP)	■	A	■	B	C	D							
Risk Management Criteria (ECC)	■	■	A			B	C						
Risk Identification (API)	■	■	■	A	■	B	C	D	E				
Risk Analysis (APA)	■	■	■	■	A	■	B	C					
Risk Evaluation (APV)	■	■	■	■	A	■	■	B	C				
Selection of treatment option (TSO)	■	■	■	■	A	■	■	■	B	C			
Elabration of treatment Plan (TEP)	■	■	■	■	A	■	■	■	■	B	C		
Implementing Treatment Plan (TMP)	■	■	■	■	■	A	■	■	■	■	B	C	
Monitoring and Review (SR)	■	■	■	■	■	■	A					B	C
Recording (Eng)	■	A	B	C									
Method	average values												

Area	0	1	2	3	4	5	6	7	8	9	10	11	12
RM principles (PRM)	■	A	B	C									
Mandat and commitment (ME)	■	A	B										
Design of framework (CCO)	■	■	A	B	C	D	E						
Risk Management Implementation (MOE)	■	■	■	■	A		B	C					
Monitoring and Review (SRC)	■	■	■	■	■	A			B	C			
Continual Improvement (ACC)	■	■	■	■	■	■	A			B	C		
External context (ECX)	■	A	B	C									
Internal context (ECI)	■	A	B	C									
Process context (ECP)	■	A	■	B	C	D							
Risk Management Criteria (ECC)	■	■	A	■	■	B	C						
Risk Identification (API)	■	■	■	A	■	B	C	D	E				
Risk Analysis (APA)	■	■	■	■	A	■	B	C					
Risk Evaluation (APV)	■	■	■	■	A	■	■	B	C				
Selection of treatment option (TSO)	■	■	■	■	A	■	■	■	B	C			
Elabration of treatment Plan (TEP)	■	■	■	■	A	■	■	■	■	B	C		
Implementing Treatment Plan (TMP)	■	■	■	■	■	A	■	■	■	■	B	C	
Monitoring and Review (SR)	■	■	■	■	■	■	A	■	■	■	■	B	C
Recording (Eng)	■	A	B	C									
Method	maximum values												

Fig. 5: Overall result of the consolidated evaluations for the studied information systems

Table 4: Description of studied information systems

Information System	Activities	Charge (%)	Cost (%)	SO.1	SO.2	SO.3	SO.4	Global.SO.Co nt. ∑Soi & Soi/		IS Weight (%) Charge+cost Globale.cont). SOi/∑ (Charge
Business Information System (Bu_IS)	- All business activities	25%	30%	H			H	6	16%	24%
Customer Relationship Management Information System (CRM_IS)	- Customer relationship - Complaints request	5%	5%				H	3	8%	6%
Piloting Information System (Pil_IS)	- Monitoring of strategic objectives - Project management - Action plan - Actuarial - Management Control (cost accounting,..)	10	5	H		M		5	14%	10%
Control Information System (Ctl_IS)	- Quality - Risks - Audit - Security	15	10		M	M	M	6	16%	14%
Development Information System SI (Dev_IS)	- Marketing - Commercial - Communication New product development - Research	10	15	H				3	8	11%
Accounting Information System (Acc_IS)	General accounting	5	10			W	M	3	8	7%
Logistic Information System (Log_IS)	- Stock - Purchase - Parks Management - Physical security	10	5			M	M	4	11	9%
Human resources Information System (HR_IS)	- Recruitment - Career - Training - Mobility - Social Affairs - pay	10	10				H	3	8%	9%
Juridical Information System (Jurid_IS)	- Legal monitoring - Juridical assistance - Litigation - Conformity	10	10	M	M			4	11	10

Table 5: Global targets control objectives

Area	PRM	ME	CCO	MOE	SRC	ACC	ECX	ECI	ECP	ECC	API	APA	APV	TSO	TEP	TMP	SR	Eng
Initial	A	A	A	--	--	--	A	B	B	A	B	A	A	A	A	A	--	--
Target	A	A	A	--	--	--	C	C	D	C	D	B	B	B	B	B	B	B

Table 6: Target levels by area for the studied information systems

	Bu_IS		CRM_IS		Log_IS		HR_IS		Dev_IS		Pil_IS		Acc_IS		Ctl_IS		Jurid_IS		Global maturity level	
	T	I	T	I	T	I	T	I	T	I	T	I	T	I	T	I	T	I	T	I
ECX	3	2	3	2	3	1	3	1	3	0	3	1	3	1	3	1	3	3	3	1
ECI	3	3	3	2	3	2	3	1	3	0	3	1	3	2	3	2	3	2	3	2
ECP	5	5	5	4	5	3	5	1	5	1	5	1	5	3	5	4	5	4	5	3
ECC	6	2	6	2	6	2	6	2	6	2	6	0	6	0	6	0	6	2	6	1
API	8	7	6	5	6	3	6	3	8	3	8	3	4	3	8	5	8	6	7	5
APA	7	6	5	4	5	4	5	4	7	4	7	4	5	4	7	4	7	4	6	4
APV	8	7	5	4	6	4	6	4	8	4	8	4	5	4	8	4	8	4	7	5
TSO	9	8	5	4	9	8	9	8	9	0	9	4	1	0	9	4	9	4	8	5
TEP	10	4	4	4	10	4	10	4	10	4	10	4	1	0	10	4	10	4	9	4
TMP	11	6	6	6	11	6	11	6	11	6	11	6	1	0	11	6	11	6	10	6
SR	12	6	6	6	12	0	12	0	12	0	12	0	3	0	12	6	12	6	11	3
Eng	3	1	1	0	1	0	1	0	3	0	3	0	1	0	3	0	3	0	2	0

Table 7: Target control objectives for the studied information systems

	Bu_IS	CRM_IS	Log_IS	HR_IS	Dev_IS	Pil_IS	Acc_IS	Ctl_IS	Jurid_IS
ECX	C	C	C	C	C	C	C	C	C
ECI	C	C	C	C	C	C	C	C	C
ECP	D	D	C	A	D	B	C	D	D
ECC	C	A	B	B	C	C	--	C	C
API	E	C	A	A	E	A	A	E	D
APA	C	A	A	A	C	C	A	C	C
APV	C	A	A	A	C	C	A	C	C
TSO	C	A	C	C	C	C	--	C	C
TEP	C	A	B	B	C	C	--	C	C
TMP	C	A	A	A	C	C	--	C	C
SR	C	A	C	C	C	C	--	C	C
Eng	C	A	A	A	C	C	A	C	C

Table 8: Improvement results needed to reach the consolidated target configuration Applying the same method leads to values in Table 9

	IS 1	IS 2	IS 3	IS 4	IS 5	IS 6	IS 7	IS 8	IS 9		
Initial matrix level values (ILV)	6	6	6	6	6	6	0	6	6		
Algorithm Matrix level results (ARV)	11	6	11	11	11	11	1	11	11		
Identical improvement	10	10	10	10	10	10	10	10	10	Global effort	Algorithm Gain for TMP
values(IIV) (IIV–	4	4	4	4	4	4	10	4	4	∑ (II V- ILV) = 42	6
(ARV– ILV)	5	0	5	5	5	5	1	5	5	∑ (A RV- ILV) = 36	

Table 9: Algorithm global effort gain

	∑ (ARV- ILV)	∑ (IIV- ILV)	Algorithm effort gain
ECX	15	15	0
ECI	12	12	0
ECP	19	19	0
ECC	42	42	0
API	24	27	3
APA	17	19	2
APV	23	26	3
TSO	29	34	5
TEP	43	49	6
TMP	36	42	6
SR	69	75	6
ENG	18	20	2
	Global effort gain	34	

Discussion

In order to analyze the results of the algorithm we compare them with those of an improvement strategy distributed identically on the nine information systems i.e., if we want for example to reach a global capacity TMP.B for the TMP area, we will need to reach this capacity for each IS. For this area, the algorithm effort gain is 1 level (Table 8).

The overall gain obtained is the effort to achieve 34 steps in the maturity matrix i.e., the human and financial cost for the completion of the various actions required to achieve the control objectives described in each level.

Conclusion

Maturity models are important tools for evaluating the effectiveness and efficiency of the IS risk management system within organizations. They ensure that the integration of this discipline generates more profit than cost. Nevertheless, the results of this evaluation can only be beneficial and exploitable if it clearly defines the best improvement plan to reach the maturity levels for Bottom-up or Top-down treatment strategies.

Following the work in which we implemented the definition of a treatment plan for the Bottom-up strategy using the “Path Prerequisites” algorithm (Elmaallam *et al.*, 2018), we have presented in this paper an optimization algorithm for the definition of an improvement plan in the case of a Top-down strategy. Thus, the organization can define the axis of overall improvements for its information system risk management and use this algorithm to optimally deduce the actions to be performed for each IS.

This approach is beneficial for organizations since they deploy less effort and gain in terms of human and financial costs for improving their information system risk management maturity.

In perspective, we plan to improve the optimization solution by integrating the dependency parameters between the risk management maturities of the different studied information systems.

Author’s Contributions

Fatima Ezzahra Ettahiri and Hicham Bensaid: Participated in experiments, coordinated the data-analysis and contributed to the writing of the manuscript.

Mina El Maallam: Designed the research plan and organized the study Participated in experiments, coordinated the data-analysis and contributed to the writing of the manuscript.

Ethics

The authors assert that this publication presents a new algorithm proposed for the first time (in the considered field) and unpublished elsewhere to the best of their knowledge. This article builds upon the authors' previously published papers and, when necessary, mentions cited references in their prior publications. The article also provided proper citation for both the authors' earlier articles and the ones they relied on. Additionally, the authors consider that neither moral nor ethical issues relative to their work are to be raised.

References

Arogundade, O. T., Abayomi-Alli, A., & Misra, S. (2020). An ontology-based security risk management model for information systems. Arabian Journal for Science and Engineering, 45(8), 6183-6198. doi.org/10.1007/s13369-020- 04524-4

Settembre-Blundo, D., González-Sánchez, R., Medina-Salgado, S., & García-Muiña, F. E. (2021). Flexibility and resilience in corporate decision making: A new sustainability-based risk management system in uncertain times. Global Journal of Flexible Systems Management, 22(2), 107-132. doi.org/10.15547/tjs.2020.s.01.069

Alter, S., & Sherer, S. A. (2004). A general, but readily adaptable model of information system risk. https://repository.usfca.edu/at/100/

Carvalho, J. A. (2000). Information System? Which one do you mean?. In Information system concepts: An integrated discipline emerging (pp. 259-277). Springer, Boston, MA. doi.org/10.1007/978-0-387-35500-9_22

Elmaallam, M., Bensaid, H., & Kriouile, A. (2019). A Maturity Model for Assessing IS Risk Management Activity Considering the Dependencies Between Its Elements. Comput. Inf. Sci., 12(1), 98-111. doi.org/10.5539/cis.v12n1p98

Amraoui, S., Elmaallam, M., Bensaid, H., & Kriouile, A. (2019). Information Systems Risk Management: Literature Review. Comput. Inf. Sci., 12(3), 1-20. doi.org/10.3844/ofsp.12681

Elmaallam, M., & 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), 34. https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.662.938&rep=rep1&type=pdf

Elmaallam, M., & Kriouile, A. (2012). A model of maturity for IS risk management case study. Computer and Information Science, 5(3), 97. doi.org/10.5539/cis.v5n3p97

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

ISO, (2009-b), groupe de travail du bureau de gestion technique de l’ISO, Management du risque Principes et lignes directrices, 2009, Numéro de référence ISO/FDIS 31000:2009(F).

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

Peffers, K., Tuunanen, T., Rothenberger, M. A., & Chatterjee, S. (2007). A design science research methodology for information systems research. Journal of management information systems, 24(3), 45-77. doi.org/10.2753/MIS0742-1222240302

Poeppelbuss, J., Niehaves, B., Simons, A., & Becker, J. (2011). Maturity models in information systems research: Literature search and analysis. Communications of the Association for Information Systems, 29(1), 27. doi.org/10.17705/1CAIS.02927

Röglinger, M., Pöppelbuß, J., & Becker, J. (2012). Maturity models in business process management. Business process management journal. doi.org/10.1108/14637151211225225

Rosemann, M., & De Bruin, T. (2005). Towards a business process management maturity model. In ECIS 2005 proceedings of the thirteenth European conference on information systems (pp. 1-12). Verlag and the London School of Economics. https://eprints.qut.edu.au/25194/

Salvati, D. (2008). Management of information system risks (Doctoral dissertation, ETH Zurich). doi.org/10.3929/ethz-a-005811464

Steenbergen, M. V., Berg, M. V. D., & Brinkkemper, S. (2007, June). A balanced approach to developing the enterprise architecture practice. In International Conference on Enterprise Information Systems (pp. 240-253). Springer, Berlin, Heidelberg. doi.org/10.1007/978-3-540-88710-2_19

Steenbergen, M. V., Bos, R., Brinkkemper, S., Weerd, I. V. D., & Bekkers, W. (2010, June). The design of focus area maturity models. In International conference on design science research in information systems (pp. 317-332). Springer, Berlin, Heidelberg. doi.org/10.1007/978-3-642-13335-0_22

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

Sienou, A. (2009). Proposition d'un cadre méthodologique pour le management intégré des risques et des processus d'entreprise (Doctoral dissertation). https://oatao.univ-toulouse.fr/7835/

van de Weerd, I., & Brinkkemper, S. (2009). Meta-modeling for situational analysis and design methods. In Handbook of research on modern systems analysis and design technologies and applications (pp. 35-54). IGI Global. doi.org/10.4018/978-1-59904-887-1.ch003