Risk Management Maturity Evaluation Artifact to Enhance Enterprise IT Quality

Misael Sousa de Araujo[1], Edgard Costa Oliveira[2], Simone Borges Simão Monteiro[3] and Tharcísio Marcos Ferreira de Queiroz Mendonça[1]
[1]*Coordenação de Gestão de Tecnologia da Informação, Fundação Oswaldo Cruz, Rio de Janeiro, Brasil*
[2]*Engenharia de Software, Campus Gama, Universidade de Brasília, Distrito Federal, Brasil*
[3]*Departamento de Engenharia de Produção, Universidade de Brasília, Distrito Federal, Brasil*

Keywords: Enterprise Risk Management, IT Governance, Maturity Model, Evaluation Artifact.

Abstract: Information plays a fundamental role throughout an enterprise architecture, figuring as a strategic component to fulfill its business processes. The application of IT Risk Management models is a key success factor to reach organizations goals. However, just by adopting risk management practices is not enough to guarantee the expected benefits. Organizations face a growing need to know how efficient their business processes are, including its risk management processes, so that an efficiency degree can be stated in a determined scale, by knowing existing deficiencies, and to make an improvement plan to raise process quality and to compare its performance with other similar enterprises. Due to the diversity of maturity models and their characteristics, this paper developed a comparative study between the main maturity models of the market, in which it was possible to define, with the help of the decision technique AHP – Analytic Hierarchy Process, the process evaluation model of COBIT 4.1 to measure risk management of IT maturity in modern enterprises.

1 INTRODUCTION

It is vital to all organizations to manage risks in order to make full use of its services and processes, where information takes a very important and valuable place. Critical business processes depend on risk management strategies in order to have assets under a safe enterprise architecture. Koehler (2015) emphasizes that, whereas we have the impression that the potential benefits and risks may not differ significantly for smaller or larger organizations, the potential of an organization to concern itself with the potential impact of a technology may differ significantly with its size and IT-related maturity. According to the IT Governance Institute (2007), successful enterprises make great efforts in knowing and managing IT risks of their assets. In Brazil, the Brazilian Institute of Corporative Governance (IBGC) recommends that all organizations adopt a risk management system to control corporative risks in a preventive manner, likelihood, impacts and treatment measures. Weill & Ross (2006) consider risk management a key element of governance, and when it is not well defined and implemented, it can result on unnecessary expenses, high general costs, operations interruption, and insufficient initiatives to manage organizational performance.

Thus, we understand that IT risk management is essential to achieve the organization´s goals, but it is not enough. There is a growing need to know the efficiency of how risk is being managed within the organization. The efficiency of the risk management process is named Risk Management Maturity. The standard ISO/IEC 15504-1 (2004) recommends the adoption of a capacity and maturity evaluation process in order to allow the comparison of levels between organizations, independently of its dimension. Hopkinson (2011) states that a significant transformation of risk management capacity in an organization takes a long time, and it demands effort and time. Therefore, the risk management process evaluation of its maturity level is both necessary to understand the present situation as well as to the continuous improvement of the IT infrastructure management.

Though there has been great effort to implement risk management practices in organizations, we lack the use of methods to measure the maturity of these practices. Shahzad and Safvi (2010) say that organizations that are reaching a higher maturity level

Araujo, M., Oliveira, E., Monteiro, S. and Mendonça, T.
Risk Management Maturity Evaluation Artifact to Enhance Enterprise IT Quality.
DOI: 10.5220/0006324404250432
In *Proceedings of the 19th International Conference on Enterprise Information Systems (ICEIS 2017) - Volume 3*, pages 425-432
ISBN: 978-989-758-249-3

can better avoid risks in their initial phases of the implementation process. These organizations need to make use of existing maturity models to make these measures. The authors have identified some problems related to choosing a risk management maturity model, such as:

- A lack of criteria that helps managers choose the Best maturity model that can be applied to IT risk management;
- A considerable variety of existing maturity models, not necessarily aligned or integrated, which makes it hard to choose one of them;
- A lack of adequate instruments associated to data collection in order to do a practical evaluation of maturity models of IT risk management (Shahzad and Safvi, 2010).

This paper presents a solution proposal to evaluate IT risk management maturity of organizations, as a means to answer some of the problems described above. For this particular reason, we are seeking to reach the following objectives.

- A comparative study of maturity models such as frameworks, standards and academic models, to identify their characteristics and to help find out the best one to apply in our context;
- The selection of this particular model that can be customized for IT risk management, based on specific criteria; and
- The development of an artifact to collect and evaluate IT risk management risks based on the selected model.

This paper is structured in 3 parts, containing the main concepts used in the context, the methodology used to reach the results and our conclusions.

2 BACKGROUND

We present in this section the concept of risk, risk management process and IT governance as a clear understanding of how these elements are complementary in nature.

2.1 Risk Definition

The definition of risk, based on canonic dictionary definitions, may vary from author´s view, however, the understanding of risk basically states that it is the "hazard or hazard likelihood" or "a situation of more or less prevision of the probability of gains or losses". The ISO Guide 73 (2009) defined risks as "the effect of uncertainty in the objectives". These uncertainties shall not be strictly taken as something negative, in the contrary, they can be positive and seen as an opportunity to work in favor of reaching the organization´s goals. According to IBGC (2009), risk is "something that probably will fail" but also from the perspective of quantifying and qualifying uncertainty in regards do gains or losses. According to the Orange Book (2004), risk is defined as the uncertainty of the result of actions and events, either as an opportunity (positive risk) or as a threat (negative risk).

2.2 Risk Management

IT has then become omnipresent and essential for any business. Because of its indispensable nature, risk management has also become vital. In all domains, risk management activities must be under control (Barafort, 2016). The definition of risk management is associated with a set of a necessary activities organized to manage risks. According to ISO Guide 73 (2009), the standard that defines the vocabulary of risk management area, risk management is a coordinated set of activities to direct and control an organization in reference to its risks. Elmaallam and Kriouile (2011), state that risk management is an indispensable discipline to any organization to reach its goals. Ramos (2008) says that risk management is the process that identifies and treats risks in a systematic and continuous manner. Silveira (2010) emphasizes that risk management is one of the main functions of managerial boards within the corporative governance process. SEI – Software Engineering Institute (2010) defines risk management as a continuous process to anticipate problems, considered an important part of enterprise administration applied to the whole project lifecycle, in order to mitigate, in an effective manner, risks and its critical impacts to projects. DSIC (2013) considers that risk management is a set of processes that allow the identification and implementation of protective measures necessary to implement security measures that are necessary to minimize or eliminate risks to which information assets are submitted, in order to balance them with operational and financial costs involved. It is thus possible to find many different definitions of the risk management process.

Coso (2007) states that risk management is a process to be applied in the establishment of strategies, formulated to identify throughout the organization potential events that can affect the goals, and to manage risks in a way that they can be compatible with the organization´s risk appetite and to allow reasonable guarantee of goal achievement. We can see that despite the differences among the cited definitions, risk management is an essential part of the organizations general strategies, and its

definitions can both used for negative and positive situations. Furthermore, whereas practices of management, it is understood that the good practices of Enterprise Risk Management imply in creating synergies between risk management activities and increasing risk awareness which facilitates better operational, tactical and strategic decision-making (Oliva, 2016).

2.3 Risk Management Process

According to ISO 31000 (2009), the risk management process is the systematic application of policies, procedures and management practices to activities namely communication, consultation, context establishment, and in the identification, analysis, evaluation, treatment, monitoring and critical analysis of risks, as illustrated in figure 1.

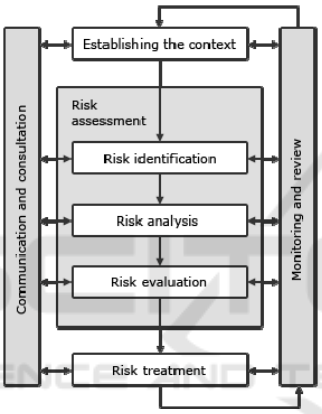

Figure 1: The risk management process (ISO, 2009).

The risk assessment activity is divided in these three activities: risk identification, risk analysis and evaluation that interacts constantly with the communication and monitoring activities, thus generation risk treatment solutions.

2.4 IT and Corporative Governance

We can consider that risk management is being adopted by organizations as part of the corporative governance, which is defined as a system to direct, monitor and incentive organizations (IBGC 2009). Corporative governance is also defined as a set of mechanisms that help corporative decisions to be taken in order to maximize business value generation perspective in a long term. Corporative governance also provides an architecture where objectives are defined and performance is fostered, established and monitored (OECD, 2004). The ISO/IEC 38500 standard of corporate governance of information technology defines governance as a system where organizations are directed and controlled (ISO, 2008). The IT governance concept is not different from the general concepts of governance, because the principles are the same: decision structure, monitoring, accountability, etc. Weill and Ross (2006) define governance as a specification of decision rights and a framework of accountability to stimulate desired actions in the use of IT. Theses authors also emphasize the importance of IT governance in the organizations by saying that a good IT governance harmonizes the decisions of the administration and the use of IT with the desired behaviors and business goals (Weill and Ross, 2006).

3 METHODOLOGY

In order to identify and select the existing maturity models, we conducted several interviews with specialists in the area, bibliographic research and content analysis. In order to define the criteria to use in the choice of a maturity model, we applied questionnaires with the IT staff involved in the context of a Brazilian IT public sector enterprise. We used a Delphi technique to obtain a reasonable consensus of the interviewees, who also analyzed the obtaining criteria. Considering tangible and intangible opinions from decision makers, we used the AHP – Analytic Hierarchy Process – a mathematical model to support decision theory (SAATY, 2009). Based in a maturity model chosen, we developed a data collection method to evaluate the maturity model that could be applied to the IT risk management process in the designed context.

4 MATURITY MODELS COMPARISON

We present here the data analysis obtained from the models selected as part of our study. We used five maturity models and frameworks available in the literature as well as existing standards: Capability Maturity Model Integration (CMMI) 1.3, Control Objectives for Information and Related Technology (COBIT) 4.1, *Formação de Valor em Sistemas de Atividades Humanas* (FVSAH), ISO/IEC 15504 standard and Risk Maturity Model (RMM).

Table 1: Resulting comparative analysis of maturity models applied to IT Risk Management.

Grouping	Characteristics	CMMI 1.3	COBIT 4.1	FVSAH	ISO/IEC 15504	RMM
Structure	Number of levels	5	6	5	6	4
	Description of maturity scales	Initial - Managed - Defined - Quantitatively Managed - Optimizing	Non-existent - Initial - Repeatable - Defined - Managed and measured - Optimized	Operation - Specialization - Growth - Convergence - Reference	Incomplete - Performed - Managed - Established - Predictable - Optimizing	Naive - Beginner - Standard - Natural
	Dependence between levels	Yes	Yes	Yes	Yes	No
Concepcion	Benchmark domain	Software Engineering	IT Control and Management	Generic	Generic	Risk management
	Evaluation tools	No	Yes	No	No	No
	Maintaining entity	SEI	ISACA	Academic (Silva)	ABNT/ISO	Academic (Hillson)
Robustness	Alignment with other documents	CMM for SW, INCOSE SECAM e EIA 731 SECM	ITIL, ISO 17799, PMBOK, PRINCE2, VAL IT, ISO/IEC 15504-1, ISO/IEC 15504-2	-	ISO 9000, ISO/IEC 2382-1, ISO/IEC 2382-20, ISO/IEC 12207 e ISO/IEC 15288	-
	Market time	7 years	6 years	2 years	5 years	16 years
Flexibility	Traceability	Yes	Yes	No	Yes	No
	Benchmarking	Dependent on external method	Native	Native	Native	Native
	Customization	Yes	Yes	Yes	Yes	No
Costs	Cost with training	$ 1300	$ 433	-	$ 300	-
	Cost with reference material	-	$ 120	-	$ 508	-

In our study, we extracted common features found in the models, grouped in five different categories: structure, conception, robustness, flexibility and costs. Based on these information, we built the comparison table (Table 1), presenting the main models characteristics. We present a group of criteria that was used to make the selection of the model, as part of the following activity. A group of five senior specialists from the analyzed context (Brazilian IT public sector enterprise) evaluated the relevance of the criteria in order to choose one of the maturity models in the context of IT risk management.

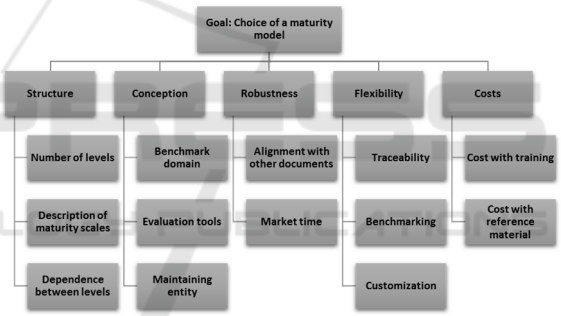

Figure 2: Hierarchical structure of used criteria to evaluate maturity models.

4.1 Criteria Structure to Use in the AHP Technique

We identified 13 criterions to categorize the features of the maturity models analyzed. This was submitted to the opinion of the specialists to obtain a relevant set of views with the help of Delphi method.

'To support the choice of a maturity model, we applied the technique AHP - Analytic Hierarchy Process - because it is a method that demands the definition of hierarchical criteria, grouped in five categories.

From this hierarchy (figure 2) it was possible to determine the structure with AHP, by taking the criteria in pairs to be submitted to comparison.

For instance, the 'structure' criteria have two others: 'level quantity', 'maturity scale description' and 'level dependency'. The comparison was made as follows:

1st comparison: quantity of levels and description of maturity scales;

2nd comparison: quantity of levels and interdependence between them;

3rd comparison: description of maturity scales and the interdependence between the levels.

We submitted the comparison table to six senior professionals who individually manifested their opinions about each criteria, in a total of 69 comparisons, which were all combined with the use of the AHP technique.

Table 2: Obtained weigh of each evaluated model.

Criteria		D = C x B x A				
N1 Criteria	N2 Criteria	CMMI 1.3	COBIT 4.1	FVSAH	ISO/IEC 15504	RMM
Structure	Number of levels	0,015	0,016	0,015	0,016	0,010
	Description of maturity scales	0,037	0,030	0,017	0,030	0,006
	Dependence between levels	0,058	0,058	0,058	0,058	0,016
Conception	Benchmark domain	0,013	0,042	0,017	0,017	0,078
	Evaluation tools	0,019	0,112	0,019	0,019	0,019
	Maintaining entity	0,007	0,022	0,006	0,031	0,006
Robustness	Alignment with other instruments	0,016	0,084	-	0,034	-
	Market time	0,009	0,012	0,004	0,011	0,007
Flexibility	Traceability	0,092	0,092	0,013	0,092	0,013
	Benchmarking	0,010	0,033	0,033	0,033	0,033
	Customization	0,037	0,037	0,037	0,037	0,020
Costs	Cost with training	0,006	0,016	0,005	0,018	0,005
	Cost with reference material	0,011	0,006	0,011	0,006	0,011

Table 3: Average weight of evaluated criteria.

Criteria				C = N3 Weights				
N1 Criteria	A = N1 Weights	N2 Criteria	B = N2 Weights	CMMI 1.3	COBIT 4.1	FVSAH	ISO/IEC 15504	RMM
Structure	0,204	Number of levels	0,199	0,358	0,389	0,358	0,389	0,253
		Description of maturity scales	0,441	0,413	0,332	0,186	0,332	0,069
		Dependence between levels	0,361	0,783	0,783	0,783	0,783	0,217
Conception	0,347	Benchmark domain	0,432	0,090	0,278	0,116	0,116	0,517
		Evaluation tools	0,377	0,144	0,856	0,144	0,144	0,144
		Maintaining entity	0,192	0,108	0,334	0,086	0,472	0,086
Robustness	0,177	Alignment with other instruments	0,754	0,119	0,626	-	0,255	-
		Market time	0,246	0,206	0,269	0,099	0,262	0,165
Flexibility	0,204	Traceability	0,516	0,872	0,872	0,128	0,872	0,128
		Benchmarking	0,207	0,226	0,774	0,774	0,774	0,774
		Customization	0,278	0,653	0,653	0,653	0,653	0,347
Costs	0,068	Cost with training	0,668	0,130	0,363	0,106	0,400	0,106
		Cost with reference material	0,332	0,485	0,253	0,485	0,262	0,485

4.2 Obtained Results from the AHP Technique

One of the main goals of the AHP technique is to make interviewees aware of the evaluated objects. However, in this research, we made a blind evaluation, by omitting to the interviewees the relationship between the evaluated criteria and the corresponding model. The reason for the blind evaluation was not to influence the opinion measure obtained and to avoid tendency choices. The results are shown in table 2.

Following the same hierarchy defined to analyze the criteria, which also have weights that define their relevance in comparison to the other criteria; we calculated the relevance of them all, based on the calculus shown in table 3 with the average weights of the criteria level 1, 2 and 3 obtained from table 2.

Table 4 presents the valued obtained in table 3 groped according to the main criterion obtained. After calculating the average of the criterion, it was possible to calculate the final scores of all models, thus indicating the preference of the interviewees to a specific model.

Table 4: results grouped by criteria level 1.

Criteria	E = Final Result (By N1 Criteria)				
N1 Criteria	CMMI 1.3	COBIT 4.1	FVSAH	ISO/IEC 15504	RMM
Structure	0,109	0,103	0,089	0,103	0,032
Conception	0,040	0,176	0,042	0,068	0,102
Robustness	0,025	0,095	0,004	0,045	0,007
Flexibility	0,138	0,162	0,083	0,162	0,066
Costs	0,017	0,022	0,016	0,024	0,016

Table 5: Final maturity models scores obtained.

FINAL SCORE OF MATURITY MODELS				
CMMI 1.3	COBIT 4.1	FVSAH	ISO/IEC 15504	RMM
0,329	0,558	0,234	0,402	0,223
19%	32%	13%	23%	13%

Based on table 5, it is possible to verify the final scores obtained for each model, resulted from the total of all average of the criteria. Cobit scores reached 0.558 points, followed by ISO/IEC 15504 with 0.0402 points and CMMI with 0.329 points. The VSAH model reached 0.234 points and RMM 0.223 points.

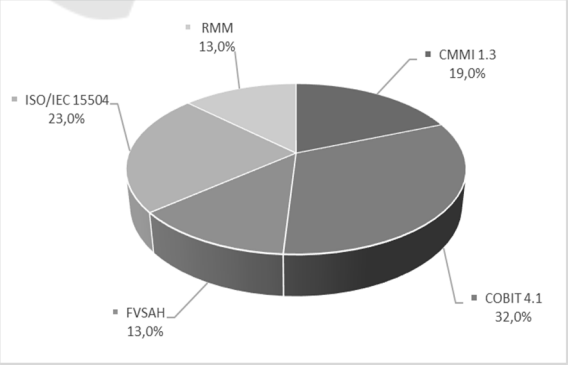

Figure 3: Maturity models interviewees preference.

The analysis of the obtained percentages of the models allowed us to identify the Cobit 4.1 framework as the adequate model to the interviewees preference, in relation to the other frameworks, and it

obtained 32% of the total scores. The second-best model was ISO/IEC 15504, with 23.0% of preferences, followed by CMMI 1.3 (18.8%) and both FVSAH (13.4%) e RMM (12.8%) as last preference.

4.2.1 Reviewing Cobit´s Reference Model

Once we defined a reference model to use, based on the multiple criteria analysis, we followed on to the development of the IT risk management maturity evaluation artifact. As we can see from the comparison made above, COBIT suggests a general evaluation template, not automated and with low levels of details. The self-assessment Cobit 4.1 guide (2011) suggests at least two instruments to help users. The first instrument is a table used to register the evaluation process results. The second one is a self-assessment model with 2 sections: one session used to register quick results of the evaluation and a second session to register detailed results. However, these sessions do not allow the customization and contextualization of criteria and process attributes. Our proposed artifact differs from Cobit´s once it has a deeper level of details, allowing the evaluation to be more specific in regards to the IT risk management process maturity level.

Cobit´s recent version maturity model is not based on CMMI anymore and is now referenced by the model established by the standard ISO/IEC 15504-2. Thus, all the original six level of maturity were kept, however they have different descriptions and meanings. The capacity levels 'incomplete', 'executed' and 'managed' have a focus the knowledge of an instance of the organizations hierarchy, while the other levels 'established', 'predictable' and 'in optimization' have their focus on the organization as a whole.

Based on these new considerations, we propose here a new artifact to evaluate IT risk management maturity in organizations, particularly to be used in the context of Brazilian public enterprises, but it can also be used by other context-related organizations.

4.3 IT Risk Management Maturity Evaluation Artifact

Our proposed artifact presents, for each evaluation criteria, a set of base practices and work products (defined based on the Cobits 4.1´s PO9 Reference Model) and associated to the level 1 and to generic practices and generic work products (based on the standard ISO/IEC 15504) and associated to the other maturity levels. Our proposed artifact differs from Cobit´s due to the fact the it's evaluation instrument presented, for each maturity level, a set of process attributes which were followed by another set of evaluation criteria.

Thus, the evaluation artifact proposed in this paper adopts 42 evaluation criteria based on the original models, and detailed in 112 new evaluation criteria, respectively associated to the maturity levels, process attributes. Table 6 describes the distribution of the new evaluation criteria per maturity model.

This new evaluation artifact, which incorporates new elements to the evaluation, allows the assessed organization to diagnosis and to answer more clearly the existence of a new practice or even a new work product, allowing the attribution of more objective answers and raising the evaluation precision.

Table 6: Evaluation criteria distributed per maturity level, process attributes and types of evidence.

Maturity Level	Process Attribute	Types of Criteria (Evidence)		Total
		Practice	Work Product	
Level 1 – Performed	PA 1.1 Execution of the process	9	14	**23**
Level 2 – Managed	PA 2.1 Execution management	6	10	**16**
	PA 2.2 Work Product Management	4	5	**9**
Level 3 – Established	PA 3.1 Process Definition	5	6	**11**
	PA 3.2 Process Implementation	6	7	**13**
Level 4 – Predictable	PA 4.1 Process measurement	6	7	**13**
	PA 4.2 Process control	5	6	**11**
Level 5 - Optimizing	PA 5.1 Process Innovation	5	5	**10**
	PA 5.2 Process optimization	3	3	**6**
Totals		**49**	**63**	**112**

As we can see on table 6, all 112-evaluation criterion are distributed by the 9 process attributes which determine the maturity level. Each process attribute has a set of evaluation criteria, which can be now grouped in 49 practices and 63 work products which help to generate evidences to reaching each level of maturity. This proposed artifact allows risk managers to register all collected work in the evaluated organization´s context as well as it automates the evaluation process.

The evaluation is based on a Yes or No question, followed by the indication if the equivalent work product is fully implemented or not.

After filling up the artifact, we must calculate the capacity index for each process attribute (1). For this particular purpose, we use the following formula:

$$PACI = \frac{QAA}{EQT} * 100 \quad (1)$$

Represented as follows:
PACI = Process Attribute Capacity Index
QAA = Quantity of Affirmative Answers
EQT = Evaluated Questions Total

After calculating the indexes for each one of the processes, it is necessary to determine the reached capacity levels, to which we use the following values. The classification N (not achieved) is used when there are no evidences of the attribute defined in the evaluation process. The P (partially achieved) is used when there is some evidence of the attribute, considering that some aspects of the attribute can be unpredictable. The L (highly reached) is used when there is evidence of the attribute in a systematic and significant way, also considering that there can be weak points related to it. Finally, the F (Fulfilled) classification is used when there is complete and systematic adherence to the evaluated attribute.

In order to define the process level of maturity, each process attribute capacity must be evaluated separately. Generally, to reach a capacity level, the evaluated process attribute must obtain the L classification (highly reached) or F (fulfilled) and its process attributes of lower level must obtain the F classification (fulfilled).

The 0 (zero – incomplete) level does not consider any process attribute. Starting from level 1, the process attributes are evaluated as requirements to a determined capacity level, which takes into consideration not only the process attributes which are required to that level, but also the process attributes of the previous level.

4.4 Validation of the Evaluation Instrument

For validation of the proposed evaluation instrument, an Excel spreadsheet was created that automates the process of calculating the percentage reached by the process attributes, also determining the level of maturity reached. The results of the application of the instrument are presented in two perspectives: analysis of the application of the instrument of maturity evaluation and results obtained by the application of the instrument of maturity.

There were difficulties in understanding some terms used in the form from level 2 criteria and difficulty was that the evaluation criteria sometimes referred to work products required by the COBIT reference model. In view of the problems reported, some changes were made to the instrument and the evaluation process.

After applying the evaluation tool, it was possible to identify that the CGTI is at level 1 of maturity (executed), and it is possible to affirm that the process reaches its purpose. For a more detailed analysis of the result, it is necessary to consult the results of the evaluations of the process attributes.

5 CONCLUSIONS

In this research, it was possible to show that the many different maturity models have distinct characteristics and goals. The comparative study presented here resulted in a comparative matrix describing in a systematic and objective form the main characteristics of these maturity models by considering perspectives of structure, conception, robustness, flexibility and costs.

Even though any of the studied models may be used as a maturity evaluation process, Cobit was the model that presented a better conformance to the defined criteria of the specialists interviewed in the context of a Brazilian public sector enterprise, based on the AHP technique. Cobit obtained the higher scores and seems to be more adequate to perform IT risk management maturity evaluation.

The application of AHP allowed the evaluation to be impartial without influencing the interviewees choices, because the compared objects were not explicitly declared, but rather they had their characteristics.

We proposed here an IT risk management maturity evaluation artifact, based on the Cobit 4.1 model. Our artifact lists 42 original criteria, expanded into 112 new criteria, allowing thus a more detailed evaluation, with more objective answers and more precision in the process attribute evaluation, but also aligned with the original criteria.

We hope that this paper allows the development of future work to broaden the research and development of new artifacts.

This research is being conducted within the master program of Applied Computing in the Computer Science Department of the University of Brasília, and our next step is going towards the application of the artifacts in the context of the public enterprises. We hope that by doing this, we will both obtain maturity levels as well as obtain a benchmarking of the evaluated enterprises.

Finally, we believe that the IT risk management evaluation process allows organizations to identify their maturity levels and to thus design an evolution plan to foster IT governance via monitoring and critical analysis in the search for improving their risk management strategies.

REFERENCES

Barafort, B., Mesquida, A.-L., Mas, A., 2016. Integrating risk management in IT settings from ISO standards and management systems perspectives. Computer Standards & Interfaces. Elsevier.

COSO, 2007, Committee of Sponsoring Organizations of the Treadway Commission.*Gerenciamento de Riscos Corporativos* – Estrutura Integrada: Sumário Executivo e Estrutura.

DSIC, 2013, Departamento de Segurança da Informação e Comunicações.*Diretrizes para o processo de Gestão de Riscos de Segurança da Informação e Comunicações.* Norma Complementar nº 04/IN01/DSIC/GSIPR. Available at: <http://dsic.planalto.gov.br/documentos/nc_04_grsic.pdf>.

Elmaallam, M. K. A., 2011.Towards a model of maturity for is risk management*, International Journal of Computer Science & Information Technology*, vol. 3, nº 4.

Hillson, D., 1997. Towards a Risk Maturity Model, *The International Journal of Project & Business Risk Management*. Vol. I, nº I, pp. 35-45, Spring.

HM Treasury, 2004. *Her majesty's Treasury.* The Orange Book, Norwich: Crown. p. 52.

Holanda, A., 2004. *Novo Dicionário Eletrônico Aurélio.* POSITIVO.

Hopkinson, M., 2011.Improving Risk Management Capability Using the Project Risk Maturity Model - a Case Study Based on UK Defense Procurement Projects, *PM World Today*., vol. XIII.

IBGC, 2009, Instituto Brasileiro de Governança Corporativa.*Código das melhores práticas da governança corporativa.* São Paulo.

ISACA, 2011, Information Systems Audit and Control Association*. COBIT Process Assessment Model (PAM)*: using *COBIT 4.1.* Illinois - USA.

ISACA, 2011, Information Systems Audit and Control Association*. COBIT Self-assessment Guide*: Using COBIT 4.1, Illinois - USA.

ISO*,* 2004, International Organization for Standardization.*ISO/IEC 15504-1:2004. Information technology – Process assessment - Part 1: Concepts and vocabulary.*

ISO, 2008, International Organization for Standardization.*ISO/IEC 38500:2008. Corporate governance of information technology*.

ISO, 2009, International Organization for Standardization. *Guide 73:2009. Risk Management- Vocabulary.*

ISO, 2009, International Organization for Standardization. *ISO/IEC31000:2009. Risk management* – Principles and guidelines.

ITGI – IT, 2007, Governance Institute. COBIT 4.1, Illinois - USA.

Koehler, J., Woodtly, R., Hofstetter, J., 2015. An impact oriented maturity model for IT-based case management. Information Systems. vol. 47, pp. 278–291, Elsevier.

Moore, R., Lopes, J., 1999. Paper templates. In *TEMPLATE'06, 1st International Conference on Template Production*. SCITEPRESS.

OECD, 2004, Organization for Economic Co-operation and Development. *Principles of Corporate Governance*. Available: <http://www.oecd.org/corporate/corporateaffairs/corporategovernanceprinciples/31557724.pdf>. Accessed (13.5.2013).

Oliva, Fabio L., 2016. A maturity model for enterprise risk management. International Journal of Production Economics 173, 66–79. Elsevier.

Ramos, A., 2008.*Security Officer, Guia Oficial para Formação de Gestores de Segurança da Informação,* Zouk. Porto Alegre.2 ed., vol. I.

Saaty, T. L., 2009.*Extending the Measurement of Tangibles to Intangibles, International Journal of Information Technology & Decision Making*, vol. 8, pp. 7-27.

SEI, 2010, Software Engineering Institute, *CMMI for Services*, Carnegie Mellon, Pittsburgh.

SEI, 2011, Software Engineering Institute. Standard CMMI A*ppraisal Method for Process Improvement (SCAMPI) A Version 1.3*: Method Definition Document, Carnegie Mellon, Pittsburgh, PA, March,.

Shahzad, B., Safvi, S., 2010.Risk mitigation and management scheme based on risk priority,*Global Journal of Computer Science and Technology.*Vol. 10, nº Issue 4, pp. 108-113, 2010.

Silva, J. M. d., 2012.*Apostila de Formação de valor em sistemas de atividades humanas*, Faculdade de Tecnologia, Núcleo de Engenharia de Produção, UnB.

Silveira, A., 2010. *Governança Corporativa no Brasil e no Mundo, Teoria e Prática,* Elsevier.Rio de Janeiro.

Vargas, R. V., 2009.*The History of Risk Management* – Based on the book Against the God. Available: http://www.ricardo-vargas.com/slides/20. Accessed (28.6.2016).

Weill, P., Ross, J., 2006.*Governança de TI: Tecnologia da Informação*, M. Books. São Paulo.