An Approach of Risk Maturity Models for SOA

Rafael Azevedo, Paulo Caetano

An Approach of Risk Maturity Models for SOA

Rafael Azevedo[1], Paulo Caetano[1]

[1]Salvador University (UNIFACS), Salvador, Bahia, Brazil.

rafael.azevedo@unifacs.br, paulo.caetano@unifacs.br

Abstract

Intensive use of Service Oriented Architecture (SOA) based technologies provides organizations with more competitiveness and transparency, but incorporates risks and challenges. Although SOA has become the primary means for the delivery and distribution of services and reuse of software components, SOA raises concerns regarding the risks to which the organization is exposed. In order to identify how organizations and academia deal with SOA risks, this paper presents a comparative study of existing risk maturity models, providing support for developing criteria for measuring and analyzing SOA risk maturity once it was not found in the literature specific risk maturity models for SOA. In addition, a literature review is presented in order to identify the state of the art on SOA risk management maturity model proposals. As a result, this paper highlights the need for a risk maturity model for SOA.

1 Introduction

Service Oriented Architecture (SOA) resembles a system with an independent set of cooperating subsystems or services. SOA encompasses the consolidation and reuse of software assets, the reduction of infrastructure complexity and, gradually, the transformation of business processes and Information Technology systems, called IT, into a set of building blocks called service. The demand for services to help build composite applications in a distributed and heterogeneous environment is increasing. The decision to adopt SOA became fundamental for companies looking for competitive market advantages, as explained by [29], through reuse, agility, and adaptability. Web Services are one of the main enablers of SOA and have become an integral part of IT systems and can help to degrade technological barriers and encourage interoperability with business partners, promoting new opportunities for interaction with customers.

With the increasing use of applications dependent on SOA and its prominent role in critical systems of the company, organizations need a comprehensive risk management strategy [29]. Security threats are now more prevalent, and a security breach can cause serious legal, economic, and corporate reputation problems. The risk management and the maturity of risk management in SOA should not be in the background and should be a relevant aspect to by establishing communication between

distributed systems. According to [29], for a successful SOA implementation, a risk management and SOA´s maturity analysis must be well defined, planned and executed.

Therefore, due to a lack of knowledge of these impacts, many companies are no longer benefiting from new technologies [9]. This can negatively affect systems development projects, that is, software development without observing practices and methodologies associated with software engineering and risk management, which could bring, with its internalization, benefits, e.g., customer service. delivery time for software projects, increased productivity of development teams, improved quality of software product, cost reduction with systems development, advances in maturity levels, risk mitigation, increased reusability, maintainability, extensibility, reliability, and testability.

In this context, the successful adoption and use of SOA is related to the transfer of IT capabilities to business processes. However, for this transfer to be assertive, it is necessary to monitor and measure the performance improvement of the processes that its services serve [17]. In this sense, the adoption of this architecture must be conducted through governed and measured activities, with the clear purpose of obtaining the maximum return on investments [17].

A relevant factor for the success of risk management is to know how much an organization consistently implements in its risk management process and its degree of maturity, as its efficiency will contribute to meeting the business objectives. Although there are several models that allow an organization to assess their level of risk management maturity, they differ in their application. Some are focused on projects, corporate governance, others on IT governance and SOA governance.

This paper presents a comparative study of existing risk maturity models, providing support for developing criteria for measuring and analyzing SOA risk maturity. In addition, a literature review is presented in order to identify the state of the art on SOA risk management maturity model proposals. As main result, this paper highlights the need for a risk maturity model for SOA.

The remaining sections of this paper are organized as follows. Section 2 describes the basic concepts used for the development of this work, and provides an analysis of the main related works identified in the state of the art. Section 3 presents a comparative analysis of the risk maturity models. Finally, final considerations and suggestions for future work are found in Section 4.

2 Background and Related Works

This section describes the fundamentals of Service Oriented Architecture and brings an overview of related works found in this research field.

2.1 Service Oriented Architecture - SOA

SOA meets the concept of service when it allows a company's business functions to be fully accessible to any of its consumers through IT components. These business functions offer a low coupling and allow total independence from the customer who is accessing the service. According to [11], Service Oriented Architecture is a technological architectural model with different characteristics to support the realization of service orientation and strategic objectives associated with service-oriented computing.

The dimensions of SOA, i.e., people, technologies and processes create artifacts that can support the implementation and use of SOA-based services. Their importance and relevance may vary from company to company, but as a good practice for building SOA solutions, all of these dimensions must be considered in an SOA adoption process, as they can contribute to the elements of risk. Like other strategic initiatives, SOA initiatives also have some considerations that are almost invariant to different business contexts or scenarios, which are these dimensions.

2.2 Related Works

This section discusses the works related to the theme of this article, i.e., the risk management maturity model in SOA. In the bibliographic research carried out, there is a lack of methods, frameworks, or models of IT risk maturity for SOA. However, proposals were identified that brought together some of the most used maturity models in the market to assess the level of capacity and maturity, and good risk management practices.

Table 1 presents a comparison of the related works found in the literature, regarding the application of risk maturity analysis, maturity models, risk maturity models, risk management and use of SOA technology.

WORKS	TYPE OF APPROACH				TECHNOLOGY
	Does it address maturity models?	Does it address risk maturity models?	Do you perform risk maturity analysis?	Does it address risk management ?	SOA
MAZUMDER (2006) [22]	NO	NO	NO	YES	YES
FILIPPOS (2011) [26]	NO	NO	NO	YES	YES
LOWIS (2010) [[20]	NO	NO	NO	YES	YES
COTFAS, et al. (2010) [8]	NO	NO	NO	YES	YES
STEFAN et al. (2008) [27]	NO	NO	NO	YES	YES
HILLSON (1997) [14]	YES	YES	YES	YES	NO
MERYEM AND LAILA (2013) [19]	YES	NO	NO	YES	YES
ARAÚJO AND OLIVEIRA (2012) [2]	YES	YES	NO	YES	NO
MAYER AND FAGUNDES (2008) [21]	YES	NO	YES	YES	NO
RIGON AND WESTPHALL (2011) [25]	YES	NO	YES	YES	NO
CHIN AND COLOMBO (2013) [6]	YES	YES	YES	YES	NO
HARRIS (2013) [13]	YES	NO	NO	NO	YES
JUNIOR, et al. (2012) [18]	YES	NO	NO	NO	YES
GERIĆ (2008) [12]	YES	NO	NO	NO	YES
CIORCIARI AND BLATTNER (2008) [7]	YES	YES	YES	YES	NO
CAMPANÁRIO, et al. (2008) [4]	YES	YES	YES	YES	NO
REN AND YEO (2012) [24]	YES	YES	YES	YES	NO
MAZZAROLO, et al. (2015) [23]	YES	NO	NO	NO	YES
ELMAALLAM AND KRIOUILE (2011) [10]	YES	YES	YES	YES	NO
CARCARY (2013) [5]	YES	YES	YES	YES	NO

Table 1: Comparison of related works

As shown in Table 1, it is possible to verify, through the analysis of the related works, that, although there are works related to SOA, allowing for a greater flexibility of the information systems, none of them covered the aspects related to the risk maturity levels in the SOA dimensions, using risk maturity models. It was also possible to verify that, although there are works that address maturity models and risk maturity models, none approached SOA technology, performing analysis and management of IT risk maturity for SOA.

3 Comparative Analysis of Risk Maturity Models

In order to make a conscious choice of the most appropriate maturity model for the analysis of risk management in SOA, some proposals were selected that will be submitted to a comparative analysis of their characteristics. The following is a brief review of these models.

For the selection of maturity models partially or in its entirety, it was necessary to identify a set of criteria that could be used for this choice, the criteria were grouped in relation to the structure, design, robustness, flexibility, and cost model. The following are criteria that should be considered when selecting the model:

- Number of levels (of the scale) of the maturity model.
- Description of the maturity scales. Names of the maturity levels identified on the scale, so that they are sufficiently clear (self-explanatory).
- Dependence between levels (need or not to fulfill the necessary prerequisites to reach a certain level).
- Domain of application of the model (adherence to the business).
- Evaluation instruments(questionnaires, spreadsheet, etc.) offered by the model.
- Maintaining entity and alignments with reference documents.
- Time of use in the market and traceability of the elements used to reach a level.
- Possibility of comparing the evaluation results (Benchmarking).
- Possibility of customizing the model for application in other domains or adapting it to an organization.
- Training costs and cost with reference material (guides, manuals, standards, etc.).

3.1 Capability Maturity Model Integration - CMMI

The Capability Maturity Model Integration - CMMI is a maturity model for process improvement. Its objective is to assist organizations in improving their product and service development and maintenance processes, through the best practices associated with activities, which cover the product's life cycle from conception to delivery and maintenance. [15].

For progression between maturity levels, CMMI uses a set of specific and generic practices associated with the process areas. To reach a level all the requirements of the previous level must be met.

3.2 Control Objectives for Information and Related Technology - COBIT

According to [16], an association linked to ISACA, which is dedicated to the advancement and international popularization of IT governance and the development and dissemination of COBIT, this is a model and a support tool that allows managers to address deficiencies with respect to the requirements of control, technical issues, and business risks, communicating this level of control to stakeholders.

The COBIT “Plan and Execute” domain consists of ten processes, one of which is the “Assess and Manage IT Risks” process. For the purposes of this work, only the PO9 process - Assess and Manage IT Risks - focus on the proposed maturity study will be considered. The control objectives of PO9 are: PO9.1 Alignment of IT and Business risk management; PO9.2 Establishment of the Risk Context; PO9.3 Event Identification; PO9.4 Risk Assessment; PO9.5 Risk Response; PO9.6 Maintenance and Monitoring of the Risk Action Plan.

3.3 Enterprise Risk Management – ERM

Enterprise Risk Management (ERM) was developed based on the corporate governance precept of the Committee of Sponsoring Organizations - COSO (2004), which determines a model for the identification, assessment, and disclosure of risks that large corporations may be exposed to. The purpose of this model is to provide guidelines for the evolution and improvement of risk management, serving as a basis for the organization to determine whether risk management is being effective, or on the contrary, what it needs to become effective.

The ERM implementation guide developed by the company Protiviti, presents a maturity model to determine the need for improvements in risk management. This model was based on the Software Engineering Institute's CMM model represented by five stages.

3.4 Value Formation in Human Activity Systems - FVSAH

This maturity model proposed by [28] is based on value formation in systems of human activities - FVSAH. The value of institutions has undergone transformations and with that, new concepts, definitions, and ideas have taken the place of physical and human resources in the production of services and products [3]. The FVSAH model has five levels of maturity, with the first level named “functioning” and the last level “reference”.

3.5 ISO/IEC 15504

The ABNT NBR ISO/IEC 15504-2 standard defines the structure and conditions for an assessment of organizational maturity based on the assessment of process capacity [1]. The standard describes the requirements for: (i) building maturity models, (ii) conducting organizational maturity assessment and (iii) verifying compliance with organizational maturity assessments.

For the purposes of this work, we will briefly define the subprocess of ISO / IEC 15504 Management Processes, “Risk Management-MAN.4” in order to address issues related to risks.

3.6 Risk Maturity Model – RMM

The Risk Maturity Model - RMM created by [14], suggests four levels of capacity named: Naïve, Novice, Normalized and Natural, which, translating into Portuguese, becomes: naive, participant, normalized and natural. The RMM allows to measure the maturity of the risk from the four areas (Culture, Process, Experience and Application), where the transition between levels occurs from the relationship of the attributes of these areas with the levels.

3.7 Analysis of Maturity Models

After describing the ERM, COBIT, RMM, CMMI, FVSAH and ISO/IEC 15504 maturity models, it is observed that, although the models were created by different entities and with different purposes. In addition, it is possible to identify that some characteristics are common among them, such as: number of maturity levels, dependence between levels, assessment, and measurement instruments.

It is also noticeable that among the models covered, COBIT is the only one to present an assessment tool (non-free), called COBIT Assessment Program, which includes the COBIT PAM (Process

Assessment Model) package where assessments can be performed based on in the descriptions of the maturity level as a whole or with greater rigor based on individual statements in the descriptions of the maturity levels. For the other models, the evaluation instrument can be developed through an evaluation questionnaire, as suggested by Hillson in the RMM model. The COBIT model also offers templates to be used or adapted for application in organizations and has in its structure, a process described for the IT risk management area that is widely used in public and private organizations.

It is also observed that some models have a more complete structure in their architecture than others regarding the approach, treatment, and assessment of risk management, being proposed in its entirety to assess the level of risk maturity, being they the model RMM and ERM.

The RMM model does not offer an assessment tool, suggests the use of an assessment questionnaire but does not exemplify or describe how a questionnaire should be developed.

The importance of CMMI is due to the fact that it is the first maturity model created in Software Engineering, in order to provide two types of representation: continuous and by stages, allowing to focus on a process in isolation and allowing to approach process improvements in stages, called degree of maturity. All other existing maturity models were developed based on CMMI, with levels of maturity in their architecture.

ISO / IEC 31000, in turn, has a clear risk management flow in its structure, but does not address levels of maturity.

The FSVAH maturity model proposes its application in any scope, focusing on the value of risks and human value in the execution and management of activities. This concern with the model and its selection is due to the need to assess the maturity of the SOA dimension “People”. As it is a generic model, it is necessary to customize it in relation to the organization's business before its application, which makes the model flexible. It was also noted that the FSAVH model does not provide mechanisms for tracing the evidence used for positioning at a certain level.

ISO/IEC 15504, in turn, is a generic maturity model with a focus on process evaluation. To perform risk management maturity assessment, it is necessary to use it combined with an external model such as the ISO/IEC 31000 standard.

Models / Description	ERM	COBIT 4.1	ISO/IEC 15504	CMMI	RMM	FVSAH
Maintainer	COSO	ISACA	ABNT/ISO	SEI	Acadêmico (Hillson)	Acadêmico (Silva)
Num. of Levels	5	6	6	5	4	5
Alignment with other instruments	ISO 31000	ITIL, ISO 17799, PMBOK, PRINCE2, VAL IT, ISO/IEC 15504	ISO 9000, ISO/IEC 2382, ISS/IEC 15288	CMM FOR SW, INCOSE SECAM, EIA 731 SECM	Not applicable	Not applicable
Rastreability	Yes	Yes	Yes	Yes	No	No
Benchmarking	Native	Native	Native	Dependent on external method	Native	Native
Customization	Yes	Yes	Yes	Yes	No	Yes

Training Cost	Yes	Yes	Yes	Yes	Not applicable	Not applicable
Maturity Levels	Level 1: Initial Level 2: Repeatable Level 3: Defined Level 4: Managed Level 5: Optimizing	Level 0: None Level 1: Initial Level 2: Repeatable Level 3: Defined Level 4: Managed and measured Level 5: Optimized	Level 0: Incomplete Level 1: Executed Level 2: Managed Level 3: Established Level 4: Predictable Level 5: In optimization	Level 1: Initial Level 2: Managed Level 3: Defined Level 4: Managed quantitatively Level 5: In optimization	Level 1: Naive Level 2: Beginner Level 3: Normalized Level 4: Natural	Level 1: Operation Level 2: Specialization Level 3: Growth Level 4: Convergence Level 5: Reference
Dependency between Levels	Yes	Yes	Yes	Yes	No	Yes
Measurement	Not addressed	Native	Native	Depends on external method	Native	Native
Domain of the Reference Model	Risk management	IT Control and Management	Generic	Software Engineering	Risk management	Generic
Assessment tools	No	Yes	No	No	No	No
Market Time	11 years	6 years	5 years	7 years	16 years	2 years

Table 2: Comparative table of the main criteria of the maturity models

Table 2 presents comparison key features of maturity models based on criteria defined in the Section 3.

4 Final Considerations

This article aimed to study the risk management maturity models for applicability in the scope of SOA. Sought to investigate the benefits of adoption of risk maturity model for SOA. For this, it made searchable to and review of the literature, in order to get answers to the purposes of this article. A comparative analysis was made of the main governance maturity models in SOA and a review of proposals for risk management maturity models for SOA. Identified that there is no maturity model in the market and academic that meets the main criteria considered in this work (Section 3) for maturity models in risk management in SOA, therefore, it is evident the need to develop a risk maturity model specific to service-oriented architecture.

From this work can be concluded that the right choice of the maturity model for managing risks in SOA brings benefits to: Corporate Governance, Governance of IT Governance SOA, auditors, to development teams and software for companies' development of SOA solutions, allowing a holistic view of the level of risk maturity in SOA in its dimensions.

As future work, the next steps are: (i) development of an instrument or method for assessing the level of risk maturity in SOA; (ii) creation of a risk maturity model for SOA, elaborated based on the studies and comparison of the risk maturity models presented in this work; and (iii) evaluation of the proposed model through a practical application in one or more organizations that have a service-oriented architecture as a software development model.

Acknowledgments

I would like to extend my special thanks to Professor Dr. André Araújo from Federal University of Alagoas for the great support and contribution in this paper.

References

[1] ABNT. (2008b). ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. ISO 73: Primeira Edição. Gestão de Riscos — Vocabulário. Rio de Janeiro: ABNT.

[2] ARAUJO, M. S. (2012). Estudo comparativo de modelos de maturidade aplicados à gestão de riscos - uma abordagem sob a perspectiva da tecnologia da informação. Acesso em 05 de Apr de 2019, disponível em http://www.excelenciaemgestao.org/Portals/2/documents/cneg10/anais/T14_0191.pdf

[3] BOLTOUN, R. E., LIBERTY, B. D., & M., S. S. (2000). *Cracking the Value Code: How success businesses are creating wealth in the New Economy.* New York.

[4] CAMPANÁRIO, M. d. (2012). Metodologia e Níveis de Maturidade em Gestão de Riscos de Projetos nas empresas de Serviços de Telecomunicações. *CONVIBRA - Congresso Virtual Brasileiro de Administração*. Acesso em 22 de May de 2019, disponível em http://www.convibra.com.br/artigo.asp?ev=25&id=1807

[5] CARCARY, M. (2013). IT Risk Management: a capability maturity model perspective. *Innovation Value Institute, National University of Ireland Maynooth*. Acesso em 11 de May de 2019, disponível em www.ejise.com/issue/download.html?idArticle=858

[6] CHIN, H. Y. (2013). Boas práticas de gestão de risco corporativo: estudo de dez empresas. Acesso em 06 de Apr de 2019, disponível em http://www2.pucpr.br/reol/index.php/rebrae?dd99=pdf&dd1=7664>. Acesso em 06 abr

[7] CIORCIARI, M. B. (2008). Enterprise Risk Management Maturity-Level Assessment Tool. *Society of Actuaries*. Acesso em 22 de May de 2019, disponível em http://jvvnz.x.incapdns.net/library/monographs/other-monographs/2008/april/mono-2008-m-as08-1-ciorciari.pdf

[8] COTFAS Liviu, P. D. (2010). Techniques for Service Oriented Architecture Applications. Acesso em 09 de Jul de 2019

[9] DEBRECENY, R. (2009). Research on IT governance, risk, and value: Challenges and opportunities. *Journal of Information Systems 27 (1)*, 129-135.

[10] ELMAALLAM, M. K. (2011). Towards a Model of Maturity for IS Risk Management. *International Journal of Computer Science & Information Technology (IJCSIT), 3*(4). Acesso em 09 de May de 2019, disponível em http://airccse.org/journal/jcsit/0811csit14.pdf

[11] ERL, T. (2009). *Service-Oriented Architecture (SOA): Concepts, Technology, and Design.* (9ª Edition ed.). Prentice Hall.

[12] GERIĆ, S. (2008). Service-Oriented Architectures Maturity Models. Acesso em 03 de Mar de 2019, disponível em https://www.mtf.stuba.sk/docs/internetovy_casopis/2008/4mimorc/geric.pdf

[13] HARRIS, T. (2013). A SOA Maturity Model. *A SOA Maturity Model.* . Acesso em 12 de Apr de 2019, disponível em http://www.thbs.com/knowledge-zone/soa-maturity-model

[14] HILLSON, D. (1997). *Towards A Risk Maturity Model.* Acesso em 19 de Jun de 2019, disponível em http://www.risk-doctor.com/pdf-files/rmm-mar97.pdf

[15] INSTITUTE., S. –S. (November de 2010). CMMI for Services. Pittsburgh, PA. Carnegie Mellon.

[16] ITGI. (2019). *ISACA.* Retrieved Apr 15, 2019, from ISACA: http://www.isaca.org/cobit/pages/default.aspx

[17] JANIESCH, C. K., & ROSEMANN, M. (2009, December 4). Conceptualisation and Facilitation of SOA Governance. *In: Proceedings of ACIS 2009: 20th Australasian Conference on Information Systems*.

[18] JUNIOR, J. J. (2012). Pontos chaves para adoção de uma arquitetura orientada a serviços: uma análise comparativa de modelos de maturidade SOA da indústria. Acesso em 27 de May de 2019, disponível em http://www.lbd.dcc.ufmg.br/bdbcomp/servlet/Trabalho?id=11327

[19] KASSOU, M. K. (2013). A Goal Question Metric Approach for Evaluating Security in a Service Oriented Architecture Context. *IEEE, Europa. 2013.* Acesso em 07 de May de 2019, disponível em http://arxiv.org/ftp/arxiv/papers/1304/1304.0589.pdf

[20] LOWIS, L. (2010). Towards automated risk identification in Service-Oriented Architectures. Acesso em 08 de May de 2019, disponível em http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.143.6303&rep=rep1&type=pdf

[21] MAYER, J. F. (2008). Proposta de um modelo para avaliar o nível de maturidade do processo de gestão de riscos em segurança da informação. Acesso em 15 de May de 2019, disponível em http://sbseg2008.inf.ufrgs.br/proceedings/data/pdf/st02_03_wticg.pdf

[22] MAZUMDER, S. (2006). A Perspective on Implementation Risks. *SETLabs Briefings*. Retrieved Jun 08, 2019, from https://s3.amazonaws.com/academia.edu.documents/44814562/soa-perspective-implementation-risks.pdf?response-content-disposition=inline%3B%20filename%3DSOA_A_Perspective_on_Implementation_Risk.pdf&X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Credential=AKIAIWOWYY

[23] MAZZAROLO, C. F. (2015). A Method for SOA Maturity Assessment and Improvement. Acesso em 21 de May de 2019, disponível em http://www.ewh.ieee.org/reg/9/etrans/ieee/issues/vol13/vol13issue1Jan.2015/13TLA1_30Mazzarolo.pdf

[24] REN, Y. T. (2012). Risk Management Capability Maturity Model for Complex Product Systems (Cops) Projects. *Center for Project Management Advancement (CPMA), School of Mechanical and Production Engineering, Nanyang Technological University, Singapore*. Acesso em 21 de May de 2019, disponível em http://www-scf.usc.edu/~yingtaor/publications/RM_CMM_SysEng.pd

[25] RIGON, E. A. (2011). Modelo de avaliação da maturidade da segurança da informação. Acesso em 20 de Apr de 2019, disponível em http://www.lbd.dcc.ufmg.br/colecoes/sbsi/2011/modelodeavalicao.pdf

[26] SANTAS, F. (Set de 2011). Mitigating Service-orientation Risk With RUP. *Service Technology Magazine, n. 54*. Acesso em 07 de May de 2019, disponível em http://www.servicetechmag.com/system/application/views/I54/0911-2.pdf

[27] SHULTE, S. R. (2008). Potential Risks and Benefits of Service-Oriented Collaboration: Basic Considerations and Results from an Empirical Study. *In: International Conference on Digital Ecosystems and Technologies – IEEE, 2008, Proceedings. Europa: IEEE, 2008.* Acesso em 31 de Mar de 2019, disponível em ftp://ftp.kom.tu-darmstadt.de/papers/SRE+08.pdf?

[28] SILVA, J. M. (2012). *Apostila de Formação de valor em Sistemas de Atividades Humanas. Faculdade de Tecnologia, Núcleo de Engenharia de Produção, UnB.* Brasilia.

[29] TIPNIS, A., & LOMELLI, I. (2009). Security – A Major Imperative for a Service-Oriented Architecture. HP. Retrieved Mar 19, 2019, from http://docplayer.net/6863478-Security-a-major-imperative-for-an-service-oriented-architecture.html