IT Risk Management Maturity Model for SOA

Rafael de Almeida Azevedo
Master Program in System and Computing
Salvador University Salvador/BA, Brazil

Paulo Caetano da Silva
Master Program in System and Computing
Salvador University Salvador/BA, Brazil

André Magno de Costa Araújo
Department of Information Systems
Federal University of Alagoas
Penedo/AL, Brazil

ABSTRACT
Risk management is an important area of knowledge in corporate environments, allowing risks to be known and adequately mitigated and addressed. A structured information technology risk management environment can influence the improvement of the flexibility and adaptability of an organization's business processes. In this context, the concept of service-oriented architecture (SOA), aims at the union of organizational processes with the resources provided by information technology (IT). Although SOA has been widely debated and applied in organizational environments, it realizes little attention has been paid to the investigation of a risk management model to assess the maturity of business processes in information technology based on SOA. This work presents a risk management maturity model, formed by the union of good information technology risk management practices and existing maturity models, to be applied in a service-oriented architecture. The proposed model aims to assist in assessing the level of risk management maturity in the SOA scope. To evaluate the proposed model, the scenario of a health organization was used, and the results showed that, the level of IT risk management maturity based on SOA was measured, which provided a holistic view of risk management on the dimensions, people, processes, and technology.

General Terms
Service Oriented Architecture.

Keywords
Maturity Models, IT Risks Maturity Models, SOA.

1. INTRODUCTION
Risk management is an important area of knowledge in corporate environments, allowing risks to be known and adequately mitigated and addressed. A structured information technology risk management environment can influence the improvement of the flexibility and adaptability of an organization's business processes [1].

Risk management in information technology (IT) has been widely debated and applied in organizational environments, this is because business processes are increasingly dependent on technological resources and tools as they expand, evolve, and become more present in the daily life of society [2]. In this context, it is necessary for organizations to implement an effective risk management process, subjecting it to continuous assessment through a maturity model appropriate to the organizational culture in question [3].

Due to the operational and strategic support provided by IT to an organization's business processes, much has been discussed about the use of maturity models that put together organizational processes with information and communication technology resources [4-5]. In this sense, service-oriented architecture (SOA), consists of a technological architectural model that aims to align IT resources with strategic organizational objectives. However, in service-oriented architecture, there is a range of components and factors that exposes this environment to a series of risks, which makes it necessary to carry out risk management, and to assess the maturity of IT risks for SOA [6].

As identified in the state of the art, IT and SOA risk management maturity models have been approached and applied in the most diverse areas of knowledge, such as healthcare [4], supply chain management [5] and e-government portal [6], among others. Although the disclosure of SOA maturity models and risk management has grown considerably in recent years [3], it is noted in the state of the art, that little attention has been paid to the specification of an IT risk management maturity model in the SOA framework and their respective sizes, which are: process, people, and technology. It is noticeable even in the state of the art that, many organizations have adopted risk management practices, however, there is a lack of studies to implement methods to measure the level of maturity organizational their practices in risk management based on SOA [7].

Based on this open issue identified in the state of the art, this work specifies an IT risk management maturity model for SOA called SDRMM (SOA Dimension Risk Maturity Model). The proposed model addresses SOA risk management in its dimensions and implements an assessment tool to measure the level of organizational maturity.

To evaluate the proposed model, a real scenario of a health institution in Brazil was used, and the main results are: the level of IT risk management maturity based on SOA was measured, which provided a view holistic approach to risk management on dimensions, people, processes, and technology.

This paper is organized as follows: Section 2 describes the basic concepts used to develop this work, while Section 3 presents and describes the SDRMM model. Section 4 show the assessment of SDRMM Model. Finally, final considerations and future work suggestions are found in Section 5.

2. BACKGROUND AND RELATED WORKS
This section contextualizes SOA (Section 2.1), conceptualizes risks maturity models (Section 2.2), and provides an analysis of related works identified both in Academia and Industry (Section 2.3).

2.1 SOA
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 [8], 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 (Service-Oriented Architecture) and its prominent role in critical systems of the company, organizations need a comprehensive risk management strategy [8]. 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 [8], 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.

Like all other strategic initiatives, SOA initiatives also have some key ingredients that are almost invariant to different business contexts or scenarios. In Figure 1, a set of key SOA elements are presented along the dimensions of Technology, People and Process. These elements quantify ‘what is SOA?’ and create some artefacts that can support implementation and use of SOA-based services. Their importance and relevance may vary from business to business, but as a best practice for building SOA solutions all these ingredients should be considered carefully. Otherwise, these ingredients can become the prime contributors to the risk elements in SOA implementations.[10]

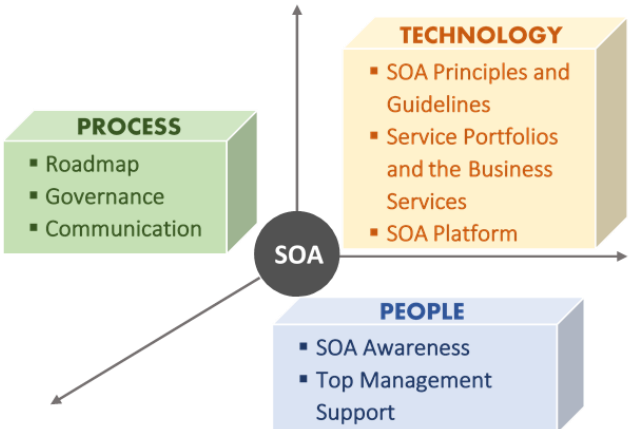


Figure 1. SOA Dimensions

A definition of each SOA dimensions is described:

Technology: SOA has its share of technology standards, principles, and best practices.

People: No SOA solution definition can be comprehensive without addressing the people aspects in it.

Process: SOA implementations, typically, span the entire enterprise and involves several internal departments, partners, and stakeholders. There must be strong processes to manage the large scope of an SOA solution.

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 [11]. 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 [11-13].

2.2 Maturity Models

Conceptually, the level of maturity can be defined as a way to continuously evaluate the performance of an organization within each discipline or group of disciplines [14]. The maturity models seek to unify the same vision, treating the evolution of maturity as stages of growth in which organizations evolve and achieve greater maturity.

A maturity model provides elements for the improvement of an organization's processes and describes an evolutionary improvement path from immature processes to mature, disciplined processes, with improved quality and effectiveness [15]. The challenge d and alignment between the areas of business s and information technology in business, highlights the need for a SOA maturity model that will enable partner organizations to assess the current state of alignment and take appropriate measures to improve it where necessary [16]. In this way, it is possible to understand maturity in risk management as an indication of the current level of capacity of an organization to execute a risk management process, describing not only its current situation, but also the necessary ways of achieving excellence from the good market practices.

In the market, there are some frameworks that insert maturity models in their contexts. The best known are COBIT - Control Objectives for Information and Related Technology (ITGI), ERM - Enterprise Risk Management- Integrated Framework (COSO) and CMMI - Capability Maturity Model Integration (SEI), among others. Although these models address risk management and risk assessment, little has been done regarding the rating level of maturity management of IT risks in a service-oriented architecture. In this context, the need for a model for this purpose is evident.

2.3 Related Works

As related works, a research of state-of-the-art studies that propose evaluation of SOA risks maturity level as well as risks maturity models has been made.

In service-oriented architecture, the maturity model was used by [17] to assess the level of maturity of the application of SOA in organizations through the use of a questionnaire, generating in the end the level of maturity in each dimension. In [16], it was used an SOA maturity model parameters and measurable criteria for measuring and assessing the effectiveness of a SOA implementation. Finally, in [18], it was discussed the need for one of risk management maturity model, there was the comparison of risk maturity models

presenting as a result the risk of maturity levels for each area/sector.

In the bibliographic research carried out, it is possible to verify, 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, performing analysis and management of IT risk maturity for SOA.

It is emphasized that the use together of risk maturity models and technology SOA is a differential in terms of benefits and contributions to resolutions of IT risk management issues for organizations using the oriented architecture services. To put this into practice, it is necessary to know the current state and level of maturity of the risks in the SOA dimensions to be able to draw up action plans and reach other levels of maturity. In this way, a safer distributed and heterogeneous environment can be aimed at in terms of reuse, agility, and adaptability, with less risk.

In the following section, is presented the proposed model.

3. SDRMM MODEL

This section presents the proposed model and is organized as follows. Section 3.1 shows an overview of Model´s Organizational Architecture and Section 3.2 discusses Compilation Risks for SOA.

3.1 SDRMM´s Organizational Architecture

This section presents the IT risk management maturity model for SOA, formed from the use of the COBIT, COSO, RMM, FVSAH(Value Formation in Human Activity Systems), ISO 15504 and ISO 31000 maturity models.

The proposed IT risk maturity model for SOA is named SDRMM (SOA Dimensions Risks Maturity Model), and its main objective is to effectively assess the level of IT risk management maturity in the SOA dimensions.

The composition of the proposed model has in its formation: (i) scale of maturity level based on the ISO 15504 standard and CMMI framework, being composed of five levels of maturity; (ii) dimension of the risk management process, based on ISO 31000, ERM COSO and COBIT, (iii) the assessment process of the SOA dimensions, which were based on the FVSAH model describing the importance of human value, characteristics, qualities, and value the risk.

As shown in **Table 1**, the SDRMM model presents levels of maturity in its structure, considering that, at each level of maturity, the SOA dimensions: people, process, and technologies and their respective subprocesses will be evaluated. To reach a subsequent maturity level, all IT risk management processes must be achieved, as well as all subprocesses in the SOA dimensions.

An organization's level of IT risk management in SOA is proportional to the way in which SOA adoption is implemented. If the use of the IT risk management maturity model for SOA is adopted since the beginning of the SOA implementation, consequently, the organization will be complying and aware of the level of maturity achieved.

Through the model it is expected to obtain visibility of the level of IT risk management maturity for SOA that the organization is in to facilitate a better definition of the scope of the SOA solution. The model will also allow the definition of a risk management method (assessment, identification, analysis, treatment of risks and communication) and management of the risk maturity level in the SOA dimensions, in addition to providing guidance on how to achieve other levels of maturity, improving the reliability of information systems and, therefore, complying with the best risk management practices. The structure of SDRMM is shown in Figure 3. In green color, is numbered the steps to perform the assessment, and in orange, is described the composition of the model SDRMM.

Table 1. SDRMM Maturity Levels Structure.

			SOA DIMENSIONS								
Maturity Level		**Maturity Level Description**	**People**		**Process**			**Technology**			
5	Optimized	IT risk management in SOA as a source of competitive advantage.	Top Management Support	SOA Awareness	Communication	SOA Governance	Roadmap	SOA Principles and Guidelines	Service Portfolios and the Business Services	SOA Platform
4	Managed	IT risks in SOA measured and managed quantitatively and the entire company involved.								
3	Defined	Defined and institutionalized policies, processes and standards.								
2	Repetitive	Continued dependence on people. Established and repeatable processes.								
1	Initial	Dependent on individual and ad-hoc attitudes. Poor institutional capacity. IT risk management in SOA not implemented.								

For the assessment of organizational risk management processes, the SDRMM model includes, in addition to the SOA dimensions, two other dimensions: process dimension and capacity dimension. The dimension of the process indicates the steps and activities that are directly mapped to the IT risk management processes in SOA. The capacity dimension describes the levels in the IT risk management maturity scale in SOA. The Initial and Repetitive capacity levels are focused on the vision / knowledge of IT risk in SOA of an instance of the organization, while the Defined, Managed and Organized levels are focused on managing the

level of IT risk management maturity in SOA in the organization.

This assessment makes the IT risk management processes evaluated in each SOA dimension, making the model more robust. As a result, the assessment demonstrates what level of maturity the organization is in, as well as what strengths and weaknesses in each area in the process dimension, facilitating decision-making and action plans so that the next level is reached.

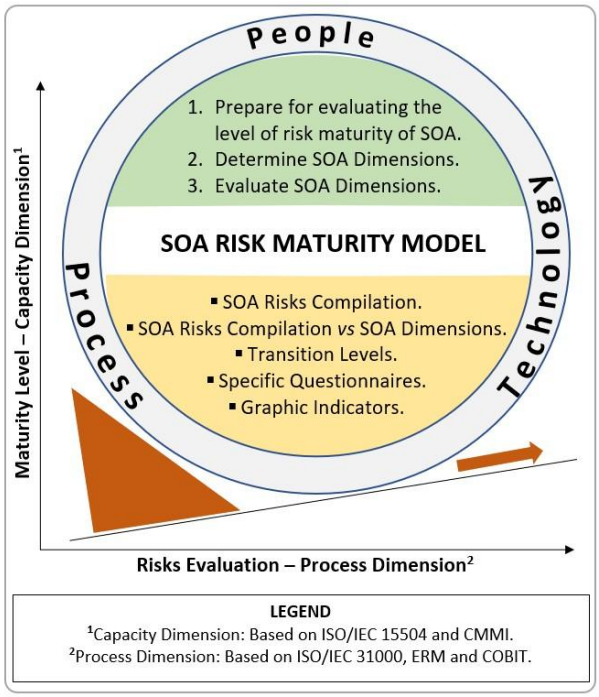


Figure 3. SDRMM Structure

The model SDRMM is divided in: (I) IT Risks Management Maturity Model for SOA, and (II) Assessment of IT Risk Management Maturity for SOA, as shown in Table 2.

Table 2. SDRMM Stages

IT RIKS MANAGEMENT MATURITY FOR SOA
Structure of the SDRMM Model
↓
Compilation of Risks in SOA
↓
Preparation of Questionnaire
⇓
ASSESSMENT OF IT RISK MANAGEMENT MATURUTY FOR SOA
Preparation for Assessing the SOA Risk Management Maturity Level
↓
Determination of SOA Dimensions
↓
SDRMM Model Application

First stage (IT Risks Management Maturity Model for SOA) is responsible for preparing the organization and adapting the IT risk management maturity model for SOA to meet the organization's needs, providing a set of activities and actions to allow the correct understanding and assessment of the maturity level of IT risk management for SOA in its dimensions.

The second stage (Assessment of IT Risk Management Maturity for SOA) is responsible for establishing the context for executing the risk management maturity level in SOA, listing a set of circumstances to permit the correct understanding of the assessment. It is expected that with the implementation of this stage, decisions will be directed to technological, people and process issues, with the purpose of conducting an organization model for SOA, contributing to the identification of the level of maturity of the management of organization's risk, in a way that allows mitigation, risk management, control of risk management maturity and reduction of unnecessary investments after the implementation of SOA.

3.2 Compilation Risks for SOA

This section presents a list of IT risks in SOA, so that the organization has knowledge about where the risk incurs in each dimension.

Table 3 lists the specific collection of risks that involve the adoption and implementation of SOA, which served to set up the traceability of the risks. The risks were organized into topics and characterized for better understanding, presented by dimension, classifying them in each SOA dimension: People, Process, and Technology. The purpose of this classification is to define which risks are directed to each dimension.

Table 3. Compilation of risks in SOA versus SOA Domains

	SOA RISKS	SOA DOMAIN
1	Difficulties in the process of developing new skills	People
2	Lack of motivation to implement reuse techniques	People
3	Lack of support from top management	People
4	Lack of effective communication with other policy makers to convince them of changing needs	People
5	Lack of effective communication between business and IT areas in the process of raising general service quality requirements for different business process scenarios	People
6	Absence of governance activities to control quality of service aspects of business processes	People
7	Lack of SOA knowledge and skill and limited knowledge of the SOA product selection committee	People
8	Ineffective communication between the SOA architect and the database architect	People
9	Improper product / platform selection due to a gap in the governance process	People
10	Lack of organizational mobility	Process
11	Management difficulties due to existing interdependent project scope and new technological risks	Process

SOA RISKS		SOA DOMAIN
12	Difficulties in ensuring quality assurance	Process
13	Waste of time in locating service information	Process
14	Absence of reliable business processes	Process
15	Mandatory standards not clearly identified with SOA principles and guidelines	Process
16	The Roadmap does not identify conflicts with other IT policies	Process
17	The SOA governance process does not provide guidelines for dealing with conflicts with other IT policies if they do not arise during the implementation phase.	Process
18	SOA principles and guidelines do not provide appropriate and / or sufficient directions for the implementation of business processes	Process
19	SOA principles and guidelines do not specify sufficient criteria for the selection of the product / platform to be used	Process
20	Absence of sufficient inputs in the SOA guidelines to define the implementation project	Process
21	Ineffective communication between the SOA architect and the infrastructure designer	Process
22	SOA governance process does not include a service implementation level review process	Process
23	SOA principles and guidelines do not provide the necessary framework for the implementation of the service	Process
24	Absence of sufficient inputs to define the error handling strategy	Process
25	Absence of defined risk management processes for SOA	Process
26	Technological deficiency to support SOA	Technology
27	Difficulty of adaptation between heterogeneous systems	Technology
28	Lack of availability and scalability within the distributed infrastructure	Technology
29	Difficulty in implementing complex system changes	Technology
30	Lack of application consistency and integrity	Technology
31	Ineffective applications due to process misalignment	Technology
32	Difficulties in reusing application features	Technology
33	Difficulties in maintaining software interoperability	Technology

4. ASSESSMENT OF THE MODEL

Is to describe the assessment carried out to validate the proposed model and is organized as follows: Section 4.1 presents the scenario in health care used in this study, while Section 4.2 discusses the application of the proposed model in setting health investigated. Finally, Section 4.3 says the main results.

4.1 Scenario Contextualization

To evaluate the model proposed in this article, the real scenario of a health institution responsible for patient care in the Brazilian health system was used.

In order to provide inpatient hospital care assisted by the Unified Health System (SUS), the Ministry of Health requires that the hospital organization providing health services be accredited with the National Register of Health Facilities (CNES), maintained by Health Care Secretariat (DATASUS). The CNES aims to regulate the services offered by each service provider, whether offered at the federal, state or municipal level. The AIH (Hospitalization Authorization) is obtained through a web system using web services. Registration data of the patient, such as SUS card number, name, sex, date of birth, affiliation, CPF and contact forms travel on the internal network and over the internet. The Hospital performs a series of transactions (sending and receiving) of sensitive patient data. Patients also access the web system for consultation of reports.

Figure 5 illustrates the communication processes and the connection between the entities involved.

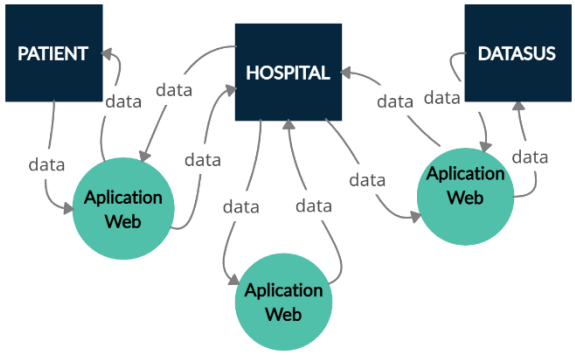


Figure 5. Communication between entities and applications

According to the scenario of health herein, the major problems reported and observed are:

(i) Low flexibility of the systems, due to the reduced capacity of the applications to be adapted to the changes that occur in legal requirements.

(ii) Sending information (transactions) through web systems using internet and web services.

(iii) Sending sensitive patient information via the network in an unsecured (non-encrypted) manner.

(iv) Several heterogeneous systems communicating via the network

(v) Difficulty in managing IT assets.

In the following section, the assessment is made through the proposed model.

4.2 SDRMM Assessment

This section aims to assess the level of IT risk management maturity for SOA in the healthcare scenario presented in Section 4.1.

As described in Figure 4, the Assessment IT Risk Management Maturity for SOA is composed by the following steps: (i) Preparation for the Assessing the SOA Risk Management Maturity Model; (ii) Determination of SOA Dimensions; (iii) SDRMM Model (apply specific

questionnaire developed by the model). Then, the results show in which maturity level the Enterprise is.

Following are the steps described above:

(i) Preparation for the Assessing the SOA Risk Management Maturity Model

The objective of this step is to establish a context for the risk assessment to produce the information that will support the decision-making process in the organization.

• Identify the purpose of the assessment

In this activity it is described how the evaluation process will be structured and carried out, through the identification of the purpose, scope, premises, and restrictions.

The objective of risk assessment is to provide an environment with efficient and effective risk management in the current software structure for service-oriented architecture, using a service bus integrated with web services. It is expected to reduce the level of threats, impacts, and determine risks of the systems environment, which directly influence the company's operations. Stakeholders are composed of business managers and information technology managers, Ministry of Health, DATASUS, the IT team, and employees. The Ministry of Health and DATASUS demand the stability of operational services; managers demand that the assessment be carried out, as well as raising the degree of IT risk management maturity to SOA quickly and efficiently in carrying out IT risk management; finally, employees and IT staff expect the performance of the service-oriented architecture to be better and more secure.

• Identify the scope of the assessment

This activity describes which levels of the organization will be approached to establish the scope and content of the assessment. At level three (information systems - technical): the organization's information systems in its operations environment are evaluated to consider the existing vulnerabilities and risks. At level two (business processes - tactical): The organization's mission and function are assessed to identify the relationship between IT risk management processes and business processes and their impact. At level one (organization - strategic): IT risks in SOA are analyzed and the IT risk management maturity level for SOA in the organization, to scale it at a strategic level.

• Identify the premises and restrictions

In this activity, the organization's restrictions and assumptions are identified to make these assumptions, risk tolerance and priorities used within the organization explicit. The organizational premises of this IT risk management is that it must be developed by the internal team, and it cannot have the intervention of external people, excluding the supporters of the SOA implementation. Organizational constraints include the period of adaptation to SOA's IT risk management, to ensure success in the implementation and leveling of knowledge among employees, issues of compatibility of the systems already existing in the organization.

• Identify sources of information

In this activity, the sources of information that provide descriptions of risks in the organization are identified. Information sources are classified as internal and external. Internal sources are risk assessment reports, incidents and security records of the company's systems and monitoring results. This information allows the current status of incidents to be identified, as well as the results of monitoring IT risks, for the purpose of detecting weaknesses in the organization. External sources of information are extracted from partners and by sharing information between systems and computer networks. This information contributes to verifying the sharing of information between the organization's security domain and the internet, to verify vulnerabilities and risks in communications.

(ii) Determination of SOA Dimensions

In this stage, the dimensions (assets involved with the adoption of SOA) of the organization are listed. These dimensions support the SOA implementation, being considered in an SOA adoption process, as they can contribute to the elements of IT risks.

• Determining of SOA Dimensions

In this activity, the critical assets of the organization are selected and categorized in the technology, people and processes dimensions. The people dimension considers awareness and skills for the adoption of SOA and support from the company's management. The technology dimension addresses SOA principles and guidelines, business portfolios and services, and ESB (Enterprise Service Bus) to ensure a scalable and adaptable SOA solution. Finally, the process dimension, which encompasses the organization and involves internal departments, partners and shareholders, who have business processes.

(iii) SDRMM Model Application

The SDRMM model has a specific questionnaire comprising risks and SOA dimensions. After applying the questionnaire, the following results were generated as shown in Figure 5.

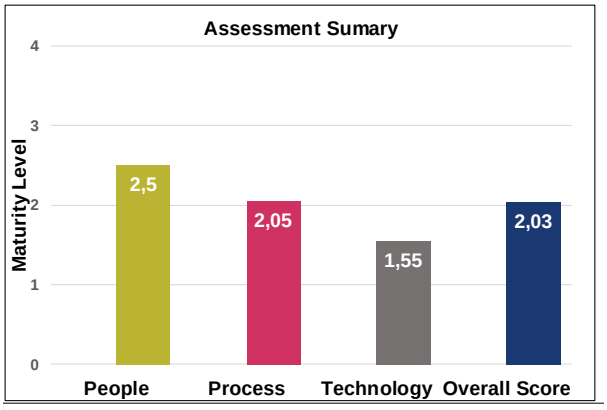
Analysis of the IT Risk Maturity Assessment in SOA

Weighted Score	2,03

MATURITY LEVEL 2: REPETITIVE

What does this mean?
Continued dependence on people. Established and repeatable processes.

	Evaluated Dimensions	Scores
Summary	People	2,50
	Process	2,05
	Technology	1,55



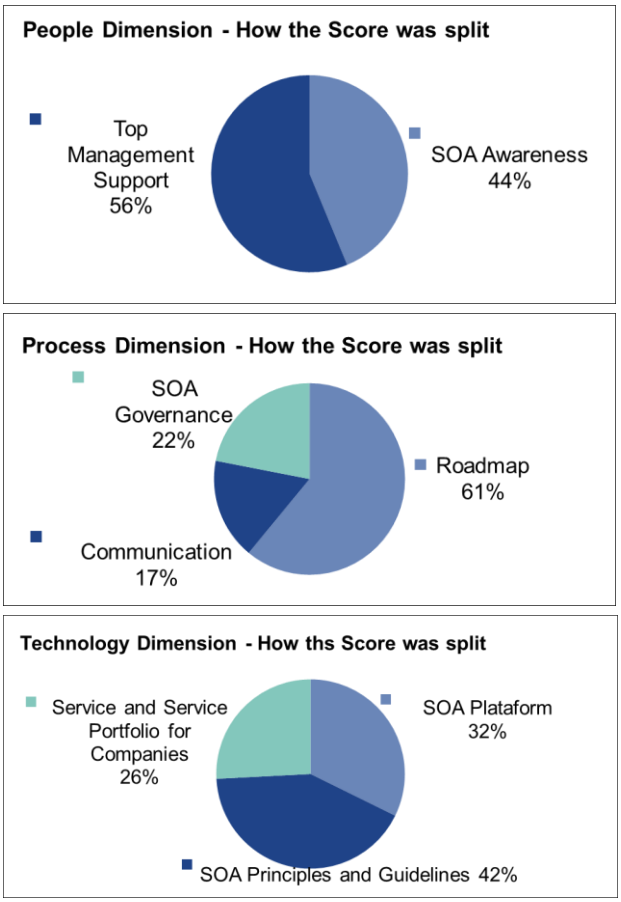


Figure 5. Result of the Assessment of Health Scenario with the SDRMM Model

The summary of the assessment points out that the organization in the health area meets the level of maturity of IT risk management at SOA at level 2, categorized as Repetitive. At this level, the organization has an immature approach to assessing IT risk management maturity for SOA with some risk management processes still being defined, and risk management is applied only in response to problems.

Characteristics of this level are:

- Concern on the part of the organization about the importance of SOA, as well as the risks inherent to its dimensions.
- There are some defined risk management processes defined for SOA.
- Existing communication in a deficient way.
- Reactive actions, still dependent on people.
- Thinking in SOA governance process.
- Existence of ESB technology in a non-scalable way, without major risk management mechanisms.
- Existence of SOA services portfolio, but there is no structure in the definition of the service versus risks and risk management.
- No risk monitoring in SOA in an efficient and continuous way.
- Little integration between IT and Business teams, making the Roadmap difficult.

The assessment also shows an imbalance between the levels of IT risk management maturity in each SOA dimension, being: Dimension People with a maturity level of 2.50, Dimension Processes with a maturity level of 2.05 and Technology with a level of equal maturity 1.55. Another point highlighted in the assessment is the score of the SOA dimensions: People, Process, Technology and percentage of their respective subprocesses, as shown in Figure 5. This imbalance reinforces the need to assess the risk management process for each dimension.

4.3 Discussion

This section describes the main results obtained in the assessment of the scenario.

As assessed by the scenario in section 4.2, the SDRMM model allows a holistic view of the risk management processes, presenting scores in each SOA dimension and percentage of its subprocesses. It is also evident the importance of the risk management process in a service-oriented architecture. Another highlight is, although the organization is at the level 2 of IT risk management maturity at SOA, there is a discrepancy in relation to the level of maturity of each dimension, thus evidencing the need to evaluate the dimension (s) with result below the value 2 (two) separately.

According to Table 4, the SDRMM model also presents a correlation of the problems reported in Section 4.1, mapping each problem to each SOA dimension and subprocesses.

Table 4. Reported Problems of the Scenario - Classification in the SDRMM Model

Issues reported in Section 4.1	SDRMM SOA DIMENSIONS							
	People		Process			Technology		
	SOA Awareness	Top Management Support	SOA Governance	Roadmap	Communication	Service and Service Portfolio for SOA Companies	SOA Principles and Guidelines	SOA Platform
(i)	✓							✓
(ii)	✓		✓				✓	✓
(iii)			✓			✓	✓	✓
(iv)				✓	✓			
(v)	✓		✓					

It is understood that the main contributions to the creation of the IT risk management maturity model for SOA are:

(i) Definition of a context for assessing IT risk management at SOA, using the Stage Assessment of the Risk Management Maturity Level at SOA.

(ii) Definition of the SOA dimensions and their subprocesses.

(iii) Definition of context for assessing the level of IT risk management maturity for SOA, through the use of a specific questionnaire for SOA.

(iv) Definition of SOA risks and classification of SOA risks by dimension.

(v) Definition of transition between levels of maturity, through activities of transition between levels of maturity.

From these contributions, it is expected to achieve the following benefits:

(i) Improve the contingency plan to deal with SOA risks and their impacts.

(ii) Improve resource allocation and budget alignment for SOA's IT risks.

(iii) Reduce IT risks in the implementation of a service-oriented architecture.

(iv) Make Stakeholders aware of the importance of the IT risk management process for SOA.

(v) Make visible to any organization, the level of maturity of IT risk management in an SOA environment.

It is concluded that the SDRMM model, being built specifically to assess the level of maturity in the SOA scope, brings in its approach processes and activities to measure effectively and efficiently the IT risks for SOA.

5. CONCLUSION

This paper aimed to present an IT risk management maturity model for applicability within the scope of SOA and its dimensions. The proposed model was built from the use of the best practices of the COBIT, ERM, RMM, FVSAH, ISO 15504, ISO 31000 maturity models, together with SOA technology.

To validate the SDRMM model, an assessment is performed in a real-world scenario in Brazilian Public Hospitals whose results shows the risks maturity level and the importance of managing risks properly.

In the application of the first stage, the SDRMM model contributed to establish a context for the risk assessment by producing information that supports the decision-making process in the organization regarding the identification of the purpose of the assessment, identification of the scope of the assessment, identification of the premises and restrictions and identification information sources. In the next stage, the organization's critical assets were selected and categorized in the SOA dimensions: People, Processes and Technology. Finally, as part of the SDRMM model are: (i) specific IT risk management questionnaires for SOA, (ii) risks inherent in SOA, (iii) classification of risks in the SOA dimensions, and (iv) migration between levels maturity.

In this way, it is possible to assess through the scenario, that the SDRMM model contributes to creating a manageable and secure corporate environment, and that it easily adapts to changes in IT security and risk management requirements for SOA.

As future investigation, it is proposed a construction of a methodology to evaluate existing maturity models.

6. REFERENCES

[1] Elmaallam, Mina. Kriouile, Abdelaziz. Towards a Model of Maturity for IS Risk Management. International Journal of Computer Science & Information Technology (IJCSIT) Vol 3, No 4, August 2011.

[2] Erl, T. Service-Oriented Architecture (SOA): Concepts, Technology, and Design. Prentice Hall, 9ª Edition, 2009.

[3] Ganapathy, K., Priya, B., Priya, B., Prashanth, V., & Vaidehi, V. (2013). SOA Framework for Geriatric Remote Health Care Using Wireless Sensor Network. Procedia Computer Science, 19(Fams), 1012–1019. http://doi.org/10.1016/j.procs.2013.06.141

[4] Cheng, J. C. P., Law, K. H., Bjornsson, H., Jones, A., & Sriram, R. (2010). A service-oriented framework for construction supply chain integration. Automation in Construction, 19(2), 245–260. http://doi.org/10.1016/j.autcon.2009.10.003

[5] Sedek, K. A., & Omar, M. A. (2013). Interoperable SOA-Based Architecture for E-Government Portal.

[6] Shazsad, Basit; Safvi, Sara Afzal. Risk mitigation and management scheme based on risk priority. Global Journal of Computer Science and Technology. Vol. 10 Issue 4 Ver. 1.0. p. 108-113, 2010.

[7] Tipnis, Ajay; Lomelli, Ivan. Security – a Major Imperative for a Service-Oriented Architecture. [S.l.]: HP, 2009.

[8] Debreceny, Roger. Research on IT governance, risk, and value: Challenges and opportunities. Journal of Information Systems 27 (1), 129-135. 2009.

[9] Mazumber, Sourav. SOA: A perspective on implementation risks. SETLabs Briefings, India, 2006.

[10] Janiesch, C. Korthaus, A.; Rosemann, M. Conceptualization and Facilitation of SOA Governance. In: Proceedings of ACIS 2009: 20th Australasian Conference on Information Systems, Monash University, Melbourne, December 4th, 2009.

[11] Josuttis, N. M. SOA in Practice: The Art of Distributed System Design (Theory in Practice). O Really Media, 2007.

[12] Marks, E. A. Service-Oriented Architecture Governance for the Services Driven Enterprise. John Willey & Sons Inc, 2008.

[13] Kerzner, Harold. Using the Project Management Maturity Model – Strategy Planning for Project Management. 2. ed. United States of America: John Wiley & Sons, 2005.

[14] SEI – Software Engineering Institute. CMMI for Services. Version 1.3. Pittsburgh, PA. Carnegie Mellon. November 2010.

[15] Harris, Torrys. A SOA Maturity Model. University of Twente. Netherlands, 2013

[16] Mazzarolo, C. F. Martins, V. A. Toffanello, A. A. Puttini, R. S. A Method for SOA Maturity Assessment and Improvement. 2015.

[17] Ren, Y.T. Teo, K. T. 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. 2012.