International Journal of Advanced Computer Technology (IJACT)
ISSN:2319-7900

A RISK MANAGEMENT MODEL FOR SERVICE-ORIENTED ARCHITECTURE

Erasmo L. Monteiro, Salvador University – Master Program in Systems and Computing, Salvador, Bahia, Brazil
Paulo Caetano da Silva, Salvador University – Master Program in Systems and Computing, Salvador, Bahia, Brazil

Abstract

The Risk Management IT has become a constant concern for organizations, due to the increase of the implementations of service-oriented architecture (SOA) and its leading role in critical business systems. Concurrently, more organizations fail to ensure safe services, resulting in inaccurate applications, configuration problems and errors. So, organizations should understand the risk analysis tailored to your needs. In this paper, we propose a solution for risk management in SOA, since it was not found in the literature a methodology that addresses the assessment of the likelihood and impact of risks, considers software assets, threats, vulnerabilities, risks, controls external and internal environments to the organization, which assists in the development of criteria for risk measurement and profiling of information assets, so that measures losses and increase control over IT environment.

Introduction

During the last decades, the system architecture has evolved in conjunction with organizations [1]. In the 60 to 80, the system architecture was solely focused on the organization, structure focused on large computers, the type and use of Mainframe systems was internal to organizations without data analysis; between 1990 and 2000, there was a shift in focus to migrating processes based on client-server architectures, through connectivity and file transfers. According to Rainer and Falk (2010) [2], distributed functions were implemented as well as the interoperability of data and real-time connectivity, providing information systems to better adapt to changes in business requirements and technology [2]. The Service Oriented Architecture (SOA) approach covers the consolidation and reuse of software assets, reducing infrastructure complexity and transformation of business processes and IT systems into a set of building blocks called service [1]. The decision to adopt SOA has become essential for companies seeking competitive advantage in the market, as explained by Tipnis and Lomelli (2009) [1], through reuse, agility and adaptability. Web services are one of the key factors of SOA and have become an integral part of IT systems.

With the increasing dependence of SOA and its leading role in critical business systems, organizations need a comprehensive security strategy [1]. Security threats today are more prevalent and a violation can cause serious legal reputation, economic and corporate. Then, the SOA security should not be in the background, but it should be an important aspect to communicate between systems. According Tipnis and Lomelli (2009) [1], if successfully implemented, the SOA security has to be well defined, planned and executed, based on the three basic principles of confidentiality, integrity and availability, because the environment is volatile, there are always new threats and new ways to combat these threats, so security policy cannot remain static, needing to be agile in their approach and countermeasures.

The SOA introduces new threats to information security and new challenges for security professionals, such as security management in open, dynamic and distributed environments, as well as deciding on strategies to identify unforeseen [3] threats. Due to these challenges, sometimes developers cannot guarantee insurance services and SOA architectures. When combined with protocols allowed through firewalls security, such as SOAP over port 80, as is common in environments of Web Services, joining the SOA architecture can become an eminent security risk. Inaccurate implementations, configuration issues and errors can lead to exploitable vulnerabilities in web services [3]. Developers and system administrators should understand the risks posed by these vulnerabilities and mitigations to consider before deployment. Some of the critical vulnerabilities that may be introduced by the Web Services are listed in Table 1.

Some security standards for web services have been proposed, according to Badr (2013) [3], of which: (i) the level of the application layer standards such as SAML (Security Assertion Markup Language) and ebXML (Electronic Business using eXtensible Markup Language); (ii) in the message layer standards such as WS-Security (Web Services Security), XML-Signature and XML Encryption); (iii) finally, transport-level implementations with TLS (Transport Layer Security) / SSL (Security Socket Layer). These standards can be applied to Web services, not being restricted to SOA and are not specific to risk management. So, other security models have been proposed to meet the requirements of SOA environment.

ISSN:2319-7900

Table 1. Vulnerabilities Web Services

Vulnerabilities	Mitigation
Injection flaws occur when the software is not properly validating input. An attacker could create malicious entries that causes the software to perform operations like web service if an attacker. As examples, we have SQL Injection and XPath Injection.	Developers should validate all parameters of the web service on the server before using them and before generating the output. The developer should not assume that clients will generate valid entries. Gateways web services are another possible mitigation that can detect these types of attacks.
XML is a standard for encoding data versatile. However, analysis of the XML data can be intensive and complex process, which can lead to safety problems. A common problem is a denial of service (DOS) against a web service. If an attacker sends an XML message with large loads, recursive content, excessive nesting or malicious external entities, a DOS may occur.	When processing XML, XML Gateways or use filters to prevent the processing of malicious messages as they may restrict the rate of messages per second, message size, the number of nested XML elements, among other things.
Attackers may steal or modify information if it is not protected in transit.	Using the most recent versions of SSL or TLS to protect the content of messages in peer transactions. Require mutual authentication between the client and the server increases the confidence level before processing the messages and usually decreases the attack surface of the service.
Web service that generates detailed fault messages are useful for developers and system administrators. However, the same messages can provide information on operating environments. This problem also affects web service using WSDL to provide a service description and interface. The WSDL (Web Services Definition Language) describes web services and how to access them. The WSDL contains available methods services and other critical and valuable information.	System administrators should configure servers to minimize information leakage not to announce details of software, removing WSDL or authenticate the user before sending the WSDL and off every detailed error messages.
Protecting a message against modification does not prevent an attacker from passing the message to a server to invoke actions several times.	Encryption and digital signatures can provide protection against eavesdropping and modification, however, if a message encrypts signed or may be intercepted, it could still be vulnerable to a replay attack. Developers can mitigate this type of attack via timestamps on messages signed.
Web Services that perform sensitive functions shall request authentication.	For any sensitive transaction, each request must be associated with an authenticated identity and each service or data shall be associated with authorization rules.

Despite the numerous solutions and safety standards for SOA environments, they are often limited to services, mechanisms for composition and generally do not consider the environment (open and dynamic) by which applications based on SOA collaborate and share information [4]. Then, a need exists for managing security risks through comprehensive and coherent definitions of security policies (security management). This article proposes a solution for risk management in SOA, using the practices of OCTAVE [5], NIST [6] and FAIR [7] to provide insurance to changes in safety requirements and corporate IT environment. The organization of this paper is as follows: in Section Risk Management of Information Security, discusses the concepts related to the management of security risks; the next section, risk assessment methodologies for SOA is carried out; in section model proposed risk management in SOA is presented the model of risk management in SOA formed from the use of NIST 800-30, OCTAVE Allegro and FAIR; and finally, we present the final considerations and conclusions.

Risk Management of Information Security

The risk can be addressed through two perspectives, according to the Project Management Institute (2013) [8]: (i) a threat that may cause negative effect on at least one goal within the project and; (ii) an opportunity, when they cause some positive effect on the project. The management of risks aims to increase the probability and impact of positive events and decrease the probability and impact of negative events. The process of assessment or risk analysis identifies security risks to a system and determines its probability of occurrence, impact, and how to mitigate this impact [8]. Risk assessment is a step in the risk management process and its weakness way to evaluate all risks in a system or organization, so that, using the output of this review, these organizations can set appropriate controls to reduce or eliminate these risks.

Methods can be used to formally prove the results of the assessment. The method for risk assessment generally consists of four steps: (i) identification of threats; (ii) identification of vulnerabilities; (iii) determination of risks and; (iv) recommendations for controls, these steps being adopted by many organizations in a process of safety assessment, not then and there a standard for assessing risk [8]. Standards such as the International Organization for Standardization / International Electro Technical Commission [9] [10] do not define the detailed steps of risk assessment, so if an organization wants to use this rule, it must set their own methodologies for risk assessment or use other methods that have been developed by other organizations [11].

There are many methods that have been developed by organizations in order to analyze the risk in IT. In this work, we select three of these methodologies, guides and compare in order to extract the benefits of them to the organization, and to investigate whether they include gaps regarding risk

ISSN:2319-7900

assessment in SOA, which are discussed in Section Risk Assessment Methodologies for SOA. Such methodologies were chosen based on academic and market acceptance and aim to improve existing infrastructure components in an organization as technologies, emerging standards and specifications. This allows organizations to centralize the creation and management of security policies, risk analysis and identify solutions. These three methods are: OCTAVE Allegro [5], NIST SP 800-30 [6] and FAIR [7].

The Operationally Critical Threat, Asset and Vulnerability Evaluation (OCTAVE), the Allegro, 2007 release, is a methodology to streamline and optimize the process of risk assessment of information security so that an organization can obtain sufficient results with a small investment of time, people and other limited resources in the context of their relationship to information, services and business process they support. This methodology differs from other approaches as it focuses primarily on information assets in the context of how they are used, where they are stored, transported and processed, and how they are exposed to threats, vulnerabilities and disruptions [5].

The National Institute of Standards and Technology (NIST) in its Publication 800-30, Revision 1, 2012, aims to provide guidance for conducting risk assessments of information systems and amplify in Publication 800-39 [6]. This guide provides guidance for performing each of the steps of the risk assessment process (preparation for the evaluation, conducting the assessment, reporting the results of the evaluation and maintenance of this review) and how risk assessments and other processes organizational complement and inform each other. NIST SP 800-30 guide focuses on risk assessment component, providing a method for organizations: (i) prepare for risk assessments; (ii) conduct risk assessments; (iii) communicate the results of risk assessment for the key personnel and organization; (iv) maintain risk assessments over time.

The Factor Analysis of Information Risk (FAIR), in its 2005 version, implements: (i) a taxonomy of factors that composes the risk of information; (ii) a method for measuring the factors that boost the risk of information, including the frequency of events of threat, vulnerability and loss; (iii) a computational environment that simulates mathematically the relationships among the factors evaluated and; (iv) a simulation model that allows us to apply the taxonomy, the method of measurement and the computational engine [7]. This methodology consists of four components: threats, assets, organization and the external environment. Thus, a scenario assessment is classified into one of these categories, their attributes or factors that contribute positively or negatively with risk.

Risk Assessment Methodologies for SOA.

The working group of the European Union Agency for Network and Information Security Agency [12] and Zambonet et al [13] has defined attributes to classify the methods and level of visibility in the market and its main features, functions and parameters to evaluate these methodologies and guides risk management. The choice of criteria for evaluation is justified by allowing general information of methodologies, which the scope of action, identification (risk assessment or risk management), the current versioning, prices for acquisition, languages addressed, the focus within the organization, level of detail required for implementation, the main stages, characteristics and classification through the factors that make up the risk (threats, vulnerabilities and assets) skills.

The ENISA (2006) classified these attributes as follows: (i) identification of the product; (ii) the scope and coverage; (iii) the point of view of users, containing the necessary standard, consultancy skills, regulatory compliance, compliance with IT standards, license type, level of maturity of the information system, coupled with those tools, technical integration of tools available, organizational integration and flexible knowledge base. The ENISA also defined two segments evaluation: (i) risk assessment methodologies, which are approaches that analyze the security of an infrastructure, identifying and selecting countermeasures and vulnerabilities; (ii) risk management methodologies that include the implementation of appropriate policies and related controls, promotes awareness, as well as monitoring and evaluation of policy and control effectiveness.

Zambonet et al (2011) presented three parameters to assess methodologies: (i) scale used (qualitative, ordinal rating (high, medium and low) and quantitative risk expressed in numbers through ratio or interval scale); (ii) factors are used to evaluate the impact and; (iii) factors and operations used to calculate risk. The author also ranked the methodologies of risk management through classes, which would be the basis on which the properties and factors are taken into consideration: class 1 consider the probability that a particular threat will engage in an attack, vulnerability and impact; class 2 assesses risk based on the impact that a threat can have on the safety requirements that were previously defined for the asset; Class 3 is typically used in audits of financial risk, which is calculated for a given period, which makes it more applicable to cost / benefit analysis and budget. It usually requires quantitative data. One application scenario for such assessments would be made to audits by insurance companies in order to create a commission and compensation schemes. The risk is evaluated for each set of threat-active. However, the term probability here wins the meaning of "successful attempts per year" and is combined with the

ISSN:2319-7900

average financial loss caused by each of these attempt to obtain an estimate of the expected annual loss in monetary terms; class 4 is generally used for safety-critical systems, where the probability that the threat is irrelevant and that the asset should be fully protected against all threats at all times and; class 5 is based on the traditional interpretation of risk analysis in security, in which there is no specific threat. Instead, only the average frequency of adverse events and their consequences are used to estimate risk levels. These approaches are common for example in risk assessment of an onboard computer of a car or other type of system where the effect of environmental factors are relevant..

A box of rating methodologies OCTAVE, FAIR and NIST SP 800-30 is illustrated in Table 2, selected from the evaluation criteria presented in this section. The main characteristics are shown in Table 2. Approach class and define the basis of which the properties and risk factors are taken into consideration as well as the scale used for respectively risk assessments. The OCTAVE is a methodology that provides content for implementation through its manuals, is defined as class 4 to be used for security policies and risk management, while the FAIR and NIST are considered class 1 by considering the evaluation of risks through the components threats, vulnerabilities and impact. The OCTAVE and NIST are qualitative, they perform the evaluation of ordinal risk, with scales (high, medium and low), while the FAIR implements quantitative numerical evaluation to measure the impact and magnitude. The skills needed to use the methodologies were defined as standard for OCTAVE and NIST, as the use of common sense and experience on the part of security professionals would be enough to deploy, use and maintain these methodologies, and defined as basic for FAIR because it requires training for leveling of knowledge about risk management. The identification, analysis, evaluation, professional management, treatment, acceptance, risk communication attributes specify the degree of fulfillment of the investigated phase methodologies, in low, medium and high scale.

Table 2. Comparison of Methodologies for Risk Management

Attributes and characteristics	Octave	Fair	Nist 800-30
Class	4	1	1
Approach	qualitative	Both	qualitative
Focus	Assessment and Risk Management	Risk assessment	Not applicable
Skills required	Default	Basic	Default
Identification of risks	Medium	Medium	High
Risk analysis	Medium	High	High
Risk assessment	Medium	High	Not applicable
Professional risk management	Medium	High	High
Treatment of risks	Medium	Medium	High
Acceptance of risk	Medium	Not applicable	High
Risk communication	Medium	Not applicable	Not applicable
Level of detail	Management and operational	Operational and technical	Operational and technical
Key concepts	Assets, threats, vulnerabilities and risks	Threats, assets, internal and external environment	Threats, vulnerabilities, risks and controls
Main features	Discusses about the balance between three aspects: technology, operational risk and safety practices	Includes a taxonomy of risk factors that make up the information, the methods used to measure such factors, calculations for measuring and even a simulation model to create and analyze risk scenarios	Attaches great importance to risk controls and reports to executives of organization on the liability and risk management
Main stages	Develop criteria for measuring risk; organization profiles of information assets; identify threats; identify risks to assets and develop mitigation approaches.	Identify the components of the scenario; assess the likely frequency of a threat; assess the magnitude of the threat; determine the frequency and probable magnitude of future loss.	Identification of risks; propose the IT environment for risks; implement security of assets; perform maintenance risk reduction activities; perform activities of risk management in system components;
Main outputs	Assets and critical requirements, vulnerabilities, security practices; Main components and current vulnerabilities; Phase Three: the critical risks, metrics and risk asset protection strategy and mitigation plans.	Identify assets, threats and events; To estimate the frequency of threats and their capabilities and the power of resistance; estimate the losses, the frequency of events and magnitude of these losses.	Recommendations list of controls and documentation of results.

The level of detail attribute evaluates the content of the documentation of the methodologies as well as the implementation type. Because the OCTAVE is more complete explanatory content in the methodology, it is the management and operational levels, while the FAIR and NIST are operational and technical. Finally, the attributes Key Concepts demonstrate the focus of methodologies, Main features illustrate the fundamental characteristics of the methodologies, Key Stages, which discusses the key steps for adoption

ISSN:2319-7900

of methodologies and finally the Main outputs, which presents the final product after implementation. You can tell by the analysis of Table 2 that the methodologies are complementary, since the OCTAVE can cover all the steps for risk management (identification, analysis, evaluation, professional management, treatment, acceptance and communication) in managerial and operational level; FAIR does not discuss about the process of acceptance and communication on risks, however, including phases analysis, evaluation and professional risk management in operational and technical level; NIST discusses in detail the operational and technical steps identification, analysis, professional management, treatment and risk acceptance, although not approaching the assessment and risk communication. The approach, the methodologies and guides, also complete, because while the OCTAVE considers assets, threats, vulnerabilities and risks, FAIR considers internal and external to the organization's environment and NIST considers the controls of risks.

Risk Management in SOA

This section presents the model of risk management in SOA formed from the use of NIST 800-30, OCTAVE Allegro and FAIR. This model is divided into 05 layers: (i) the layer defining the SOA solution; (ii) the layer process of risk assessment of SOA; (iii) the layer process of SOA risk analysis; (iv) the layer of treatment and risk acceptance of SOA and;(v) the layer of implementing the SOA solution. Through the model, to obtain a reliable implementation of SOA is expected, in addition to improving the reliability of information systems. In order to maintain the organization and understanding of the model, each layer is composed of phases. The phases have activities that can be subdivided into tasks. The Figure 1 shows the structure of the model.

The execution sequence of the layers of the proposed model was defined with the assumption that the company must have before developing SOA services, business processes defined and aligned with the organization's strategy and IT processes structured and aligned with business goals.

The order of implementation of the layers is justified, since before the secure deployment of SOA, it is necessary that decisions of high-level guidelines and essential dimensions of SOA are defined and finalized, then start the process of evaluation, assessment, treatment and acceptance risks. Although the proposed model to establish a deployment order of layers that can be used by organizations that have no political risk management, they can be run independently of each other before the implementation of SOA solution. This is important because not all companies have the need to deploy all the layers, in despite of them already have a security policy that addresses questions about organizational and business, but do not address the issues of assessment, analysis and treatment and risk acceptance. So companies that are in this context may use the layers of the model as a reference to mature their practices and develop new initiatives.

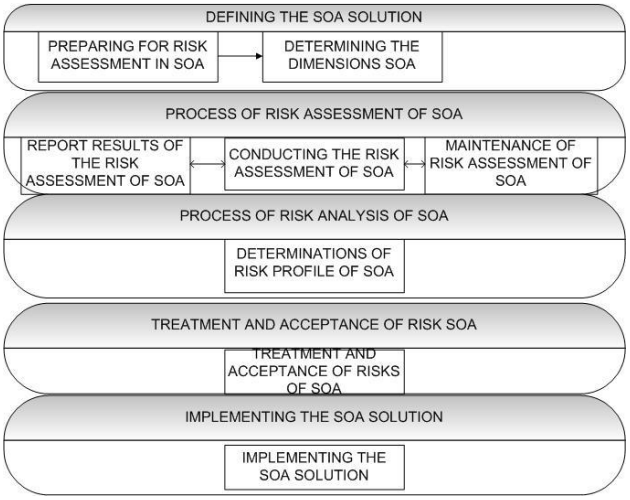

Figure 1 - Architecture of the Model Risk Management in SOA

The main objectives of the five layers that make up the proposed model are:

(i) **Layer Defining the SOA solution**: this layer is proposed to define the high-level decisions and necessary guidance on the dimensions of SOA, technology, people and processes, in order to shape the final state of the enterprise SOA environment because it would be very costly for the organization to change these guidelines and decisions at a later stage. For this, the aspects of the establishment of a framework for risk assessment through the tasks of identifying the purpose, scope, assumptions, restrictions and sources of assessment information are discussed. Also discussed will be the dimensions of people, technologies and processes that define SOA, supporting the implementation and use of services. The importance and relevance of these dimensions can vary from company to company, but as good practice for defining the SOA solution, all these dimensions must be considered. Otherwise, it can become major contributors to the elements of risk in implementations of SOA. The layer is divided into two phases: (i) the preparation for the assessment of risks in SOA that describes how the process of risk assessment will be structured and performed by identifying the purpose, scope, assumptions and constraints, sources of information, analytical approach and consists of five activities: (1) identify the purpose of the assessment, that identifies the purpose of the risk assessment in terms of the information that the evaluation was intended to have and the decisions that the evaluation is intended to support. ; (2) identify the scope of the evaluation, identifies the scope of the risk assessment in terms of organizational applicability, structure supported time and architectural considerations and technology; (3) identify assumptions and constraints associated with the evaluation, clarify the specific assumptions, constraints, risk

ISSN:2319-7900

tolerance and priorities used within organizations in order to make operational decisions and investments; (4) identify the sources of information to be used as inputs to the assessment and to determine the relevance of information of threat and vulnerability; (5) identify the risk model and analytical approach in which organizations must define one or more risk models for use in conducting risk assessments and identify which model to use for this review and; (ii) determining the Dimensions SOA phase, in order to show the dimensions of SOA. These dimensions quantify the significance of SOA and create artifacts that can support the implementation and use of services based on SOA it is composed of three activities: (1) definition of the size people, aspects requiring awareness and set of SOA skills and support to senior management, are addressed ; (2) definition of the size technology, with considerations on the principles and guidelines of SOA, portfolios / Business and Enterprise Service Bus (ESB) services; (3) definition of the size process, compounds of SOA governance and communication components. The phases and their activities are illustrated in Figure 2;

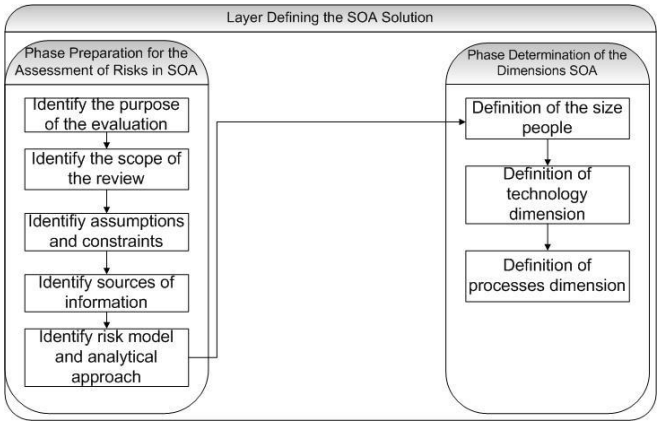

Figure 2 – Layer Defining the SOA Solution

(ii) **Layer Process of Risk Assessment of the SOA:** This layer aims to produce a list of information security risk that can be prioritized by risk level and used to inform decisions on risk responses, communicate the results of this evaluation and share information related to the risk, in order to ensure that decision makers have information related to the risk that is needed to guide decisions. Finally, this layer also aims to maintain the expertise of organizations where the risk incurred.

The layer is divided into three phases: (i) carry out risk assessment of SOA, composed of six activities: (1) identify the sources of threats that are relevant for organizations; (2) identify the threat events that could be produced by these sources; (3) identify vulnerabilities within organizations that could be exploited; (4) determine the probability of events of the threats and the likelihood that these events are successful; (5) determine the negative to organizational operations, assets and impacts; (6) determine the risks of information security, including all associated uncertainties; (ii) phase to communicate the results of risk assessment of SOA, composed of two activities: (a) communicate the results of risk assessment and; (b) share the information developed in the implementation of the risk assessment, to support other risk management activities; finally, (iii) maintenance phase of the risk assessment of SOA, composed of two activities: (1) monitor the identified risk factors and understanding these factors and subsequent amendments; (2) updating the components of risk assessments that reflect the monitoring activities performed by organizations. Phases and tasks are illustrated in Figure 3.

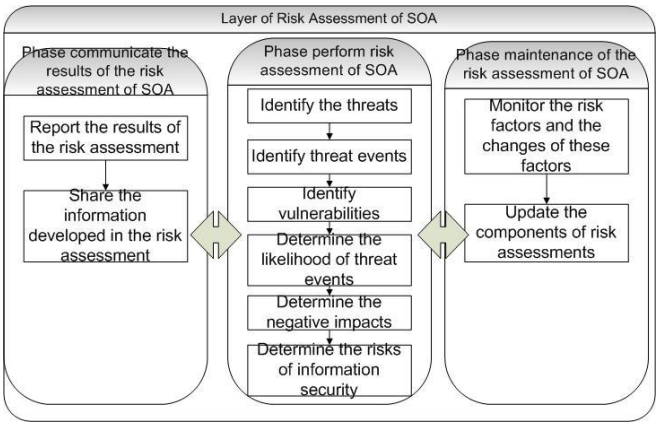

Figure 3 – Layer of risk assessment of SOA

(iii) **Layer Process of Risk Analysis of SOA**: this layer aims to establish a list of all possible risks, reporting of potential causes and likely consequences; performing qualitative and quantitative risk analysis. The tasks and phases are illustrated in Figure 4. This layer is divided when determining the risk profile, for the purpose of carrying out the identification of the risks assessed in the earlier stages, define a taxonomy that is consistent with the organization, performing risk analysis and define strategies for risks and select the approach for mitigating and composed of two tasks: (i) risk identification. The risk identification indicates the nature and scope of this identification, which may be held by or for individual business processes or systems on an aggregate level and; (ii) risk analysis. Risk assessments tend to cover a broader context that includes processes and technologies that identify, evaluate and report on issues related to risk;

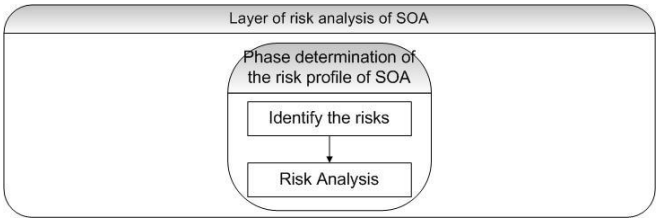

Figure 4 – Layer of risk analysis of SOA

ISSN:2319-7900

(iv) **Layer Treatment and Acceptance of Risk SOA**: this layer aims planning risk responses in order to develop options and determining actions to enhance opportunities and reduce threats to the objectives of the SOA project, and for each risk should be selected strategy or combination of strategies most likely to be effective and develop specific actions to implement this strategy. The layer also aims at monitoring and control identified, residual and new risks, keeping updated list of risks and assessing the effectiveness of actions taken. This layer is composed of phase treatment and risk acceptance of SOA. The purpose of this phase is to proceed with planning for response to negative and positive risks and carry out the contingency plan and perform the monitoring and control of risks and it is composed of two tasks: (1) planning risk responses. The purpose of this task is to develop options and determine actions for the risks. For each risk, organizations should select the strategy or combination of strategies most likely to be effective, to then develop specific actions to implement this strategy. As a result, it generates a list of residual risks and a list of secondary risks. Organizations should select the best strategy for each type of risk (negative and positive if necessary); (2) establishment of monitoring and controlling the SOA risks. Understanding where the effect of a control can be accomplished within the taxonomy is fundamental in order to accurately account for a control on an analysis. The tasks and phase of this layer are illustrated in Figure 5;

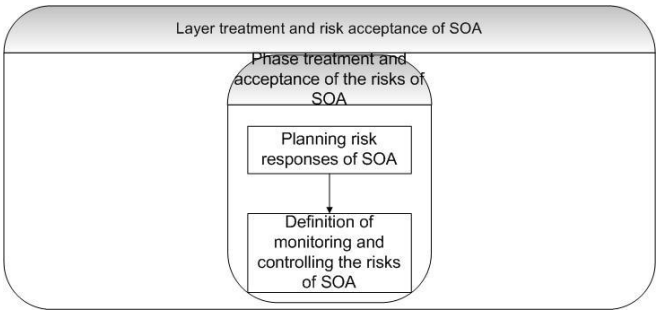

Figure 5 – Layer treatment and risk acceptance of SOA

(v) **Layer Implementing the SOA solution**: this layer proposes the secure deployment of SOA through the perspectives of the risks of business, information, application and technical architecture. This layer consists of phase implementation of the SOA solution with the purpose of demonstrating the possible risks that may arise due to poor definition of the requirements of the SOA solution and composed by the task secure deployment of SOA. A good definition of requirements and planning how it will secure SOA implementation should be performed in layer 1 of the model, in order to avoid the incidence of new risks in the implementation phase. So, it is necessary that the organization before implementing SOA, has a consistent definition of the approaches, tools, data sources that can be used to perform this implementation, roles and responsibilities, defining leadership, support and participation of team technology and risk management in each type of activity of this implementation and budgeting, usually omitted, estimates the costs required for implementation. The Figure 6 shows the phase and tasks of this layer.

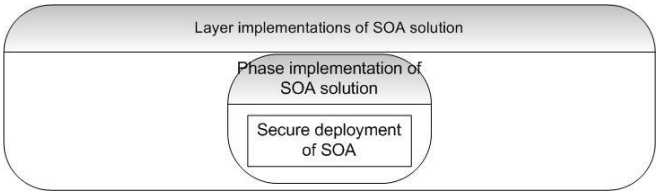

Figure 6 – Layer implementations of SOA solution

The model presented is divided into five layers with the purpose of provide a safe and free of risk enterprise IT SOA environment, helping to provide more reliable information exchange at it is SOA framework. The layer one, defining the SOA solution, showed how to plan, define requirements and identify the dimensions of SOA. In the layer two, risk assessment of the SOA, has been demonstrated to proceed with the process of risk assessment of SOA, as well as the realization of the communication of the results of this evaluation in a continuous manner and performing it maintenance throughout the lifecycle the solution SOA, keeping senior management aware of the procedures adopted. In the layer three, risk analysis of the SOA, has been demonstrated to proceed with the analysis and prioritization of identified risks using qualitative and quantitative approaches and the possibility of developing taxonomy of risks ideal for every organization. At the layer four, the treatment and risk acceptance of SOA, demonstrated how to plan responses to identified risks, as well as strategies for defining actions and monitoring of risk controls at some stages of the taxonomy. Finally, the layer five, SOA implementation solution, analyzed some risks that may affect the timing of implementation of SOA implementation, which can disrupt the organization's goals, even after the filter of the previous model layers.

Final Considerations and Conclusion

In this work were discussed concepts related to risk management, together with the methodologies OCTAVE, FAIR and the NIST guide to creating a safe environment for adoption of a service-oriented architecture and a model of risk management for SOA.

With the use of this model is expected to increase the probability and impact of positive events and decrease those that are adverse to the project implementing SOA. After analyzing the methodologies of risk management is evidenced the need to use all of these methods in order to solve

ISSN:2319-7900

the problems of risk management for SOA, since the methods have benefits, restrictions and distinct focus, for while the OCTAVE defines assets as people, hardware, software, and information systems and is a set of tools, techniques and methods for risk-based strategic assessment and planning, the objective FAIR allows organizations to have a common sense about risk in order to apply the understanding, analysis and measurement of risk information to any object or asset and NIST describes a series of activities related to risk management of the organization, through categorization of information, implementation, evaluation and monitoring of security controls.

At layer one, definition of SOA solution, the concepts and definitions of the NIST 800-30 guide in preparing for the assessment phase were used in order to enable the organization to set a context for the risk assessment, enabling the definition of the purpose of review, define the sources of information, assumptions and restrictions of the assessment. This is important for the next stage, because we need to identify the assets and sources of information, according to the OCTAVE Allegro methodology, and define them into categories, which are called dimensions.

At layer two, the process of risk assessment of SOA concepts NIST 800-30 guide were again implemented at all stages, because this guide to provide a list of risks that SOA can be prioritized by level and used to inform decisions on risk responses, ensure that decision-makers throughout the organization have the necessary information related to risk through the activities of reporting the results of the risk assessment and information sharing developed in the implementation of risk assessment to support other related to risk management and maintain risk assessments to incorporate the changes detected by continuously monitoring the existing risk assessments, understand the subsequent changes to these factors and update the components of risk assessments that reflect the activities of monitoring activities conducted by organizations.

In layer three, risk analysis of SOA, the concepts of FAIR and OCTAVE methodologies have been introduced in order to secure a list of all possible risks, reporting of potential causes and likely consequences; performing qualitative and quantitative risk analysis. The OCTAVE is used in the process of identifying risks to document the consequences of threats where those occur, as a threat may have several potential impacts on an organization, such as the interruption of the electronic trading system of an organization can affect the organization's reputation with customers as well as its financial position. The activities involved in this step ensure that the various consequences of risk are captured. The FAIR methodology is used in the phase of risk analysis to identify the assets at risk and the community of the threat that we must consider, estimate the likely frequency of the events of the threat estimate the capacity of the threat estimate the strength of the controls, deriving the vulnerability to derive the frequency of loss events, estimating the loss in the worst case and the case, and likely finally derive and articulate the risk is implemented and the taxonomy create a risk scenario for each organization.

In layer four, treatment and risk acceptance of SOA, the concepts of the OCTAVE methodology are applied in the planning phase risk response in order to select the best strategy for the identified risks and risk mitigation approaches and definition phase of monitoring and control of risks, the concepts of FAIR and NIST 800-30, were used to ensure constant monitoring of identified risks, as well as new risks and ensure control over them.

Finally, the last layer, implementation of SOA solution for good practice requirements definition and planning as will secure SOA implementation are discussed, must be held in one of these layer model, in order to avoid the incidence of new risks in the implementation phase.

Therefore, a model for risk analysis methodologies based on NIST SP 800-30, OCTAVE Allegro and FAIR in order to address the weaknesses of risk management for SOA was proposed.

References

[1] TIPNIS, Ajay. LOMELLI, Ivan. Security – a Major Imperative for a Service-Oriented Architecture. 2009, http://ebookbrowsee.net/security-a-majorimperative-for-ansoaarchitecture-pdf-d262362887.

[2] FALK, Kohlmann. RAINER, Alt. The Impact of Service-Oriented Architecture on Business Networkability. 2010, http://is2.lse.ac.uk/asp/aspecis/20100081.pdf.

[3] BADR, Youakin. BIENNIER, Frederique. NASSAR, Pascal. BANERJEE, Soumya. Challenges of Security Risks in Service-Oriented Architectures. 2013, http://liris.cnrs.fr/cyber/slides/Y-Badr-Challenges-of-Security-Risks-in-Service-Oriented%20Architectures.pdf.

[4] National Security Agency (NSA). Service Oriented Architecture Security Vulnerabilities – Web Services. 2007, http://www.nsa.gov/ia/_files/factsheets/SOA_security_vulnerabilities_web.pdf.

[5] OCTAVE ALLEGRO. OCTAVE Allegro Method. 2007, http://www.cert.org/resilience/products-services/octave/octave-allegro-method.cfm.

[6] NIST Special Publication 800-39. 2011, http://csrc.nist.gov/publications/nistpubs/800-39/SP800-39-final.pdf.

[7] JONES, Jack. An Introduction to Factor Analysis of Information Risk (FAIR). 2006, http://riskmanagementinsight.com/media/documents/FAIR_Introduction.pdf.

ISSN:2319-7900

[8] Project Management Institute (PMI). A guide to the Project management body of knowledge (PMBOX guide), Fifth edition, 2013.
[9] ISO/IEC 27001:2013. Sistemas de Gestão de Segurança da Informação - Requisitos. 2013, http://www.iso31000qsp.org/2013/11/seguranca-da-informacao-conheca-nova.html.
[10] ISO/IEC 27002:2013. Código de Prática para Controles de Segurança da Informação. 2013, http://www.abntcatalogo.com.br/norma.aspx?ID=306582.
[11] GAIVEO, Manuela. Análise e Gestão do Risco em Segurança da Informação. 2007, http://www.sinfic.pt/SinficWeb/displayconteudo.do2?numero=24868.
[12] European Union Agency for Network and Information Security (ENISA). Inventory of Risk Management – Risk Assessment methods and tools. 2005, http://rm-inv.enisa.europa.eu/tools/t_gstool.html.
[13] ZAMBON, Emmanuele, ETALLE, Sandro, WIERINGA, Roel e HARTEL, Pieter. Model-based qualitative risk assessment for availability of in infrastructures. Softw, Syst, Model., 10(4):553-580. 2011.

Biographies

ERASMO L. MONTEIRO received the BS degree in Management of Information Technology from the University AREA 1 / Ruy Barbosa, Salvador, Bahia, in 2010, postgraduate in security of computer networks by the university AREA 1, Salvador, Bahia, in 2011, postgraduate in project management for college Estacio de Sa and FIB, Salvador, Bahia, in 2013 and is currently finalizing the MS in Computer Science, Salvador, Bahia, with completion scheduled for December 2014. Currently, associate teacher of the National Apprenticeship Service Industrial - SENAI-BA, through areas of teaching and research in computer networks, network security and operating systems. This author can be contacted via e-mail erasmoleitemonteiro@gmail.com.

PAULO CAETANO DA SILVA received the PhD in Computer Science from the Federal University of Pernambuco (UFPE), Professor of the Master Program in Systems and Computing, University of Salvador - UNIFACS, Analyst at the Central Bank of Brazil, Member of XBRL International Certification Board. Organizer and author of the books "XBRL – Conceitos e Aplicações", "A Divulgação de Informações Empresariais (XBRL – eXtensible Business Reporting Language)" and "Certificação Digital – Conceitos e Aplicações" and many papers. Held several lectures and courses on XBRL in institutions such as Rutgers Business School, Central Bank of Argentina, Argentina Stock Exchange, Central Bank of Uruguay and Brazil, Comptroller of the City of Rio de Janeiro, Brazilian Federation of Banks, Faculty of Economics and Administration, University of São Paulo, II Latin American Congress of XBRL, XBRL - sponsored by Spain, in Santiago de Chile, Bolsa de Comercio de Buenos Aires, XBRL International Conference / IFRS. Contributor as a XBRL specialist at the SICONFI project on National Treasury of Brazil. Dr. Paulo Caetamno da Silva may be reached at paulo.caetano@pro.unifacs.br