American Journal of Scientific Research
ISSN 2301-2005 Issue 76 September, 2012, pp.114-132

http://www.eurojournals.com/ajsr.htm

A New Model for Information Security Management in Service-Oriented Enterprise Architecture

Safiollah Heidari
Corresponding Author, Master of Information Technology Management
Information Technology Department
Khajeh Nasir Toosi University of Technology, Vanaq Square, Tehran, Iran
E-mail: safi.heidari@sina.kntu.ac.ir
Tel: +98-936-5711179

Shahriar Mohammadi
PhD, Assistant Professor, Information Technology Department
Khajeh Nasir Toosi University of Technology, Vanak Square, Tehran, Iran
E-mail: mohammadi@kntu.ac.ir

Abstract

More complex world of business and expanding trade relationships have led to new ideas for organizations and their relationships. On the other hand, infrastructure improvement in the area of software, hardware, networks and Internet, create complex information systems to meet human needs with accuracy in a variety of fields. One of the relatively new technologies is service-oriented architecture. When we discuss the use of this technology in organizations, a new concept called service-oriented enterprise architecture (SOEA) is established. The use of SOEA is considered by global companies in recent years, and each of them tries to implement his idea in this field to get a head of other companies. However, the point that is often neglected is how to manage information security in SOEA. Security is a controversial issue in this type of architecture that directly affects on how the technology influences the productivity. So, a comprehensive model can be useful in order to implement this type of architecture. In this research, a new model for managing information security in SOEA is presented. This model can help to system designers, planners, senior managers and IT managers to manage information security in their service-oriented enterprise containing the main requirements in organizations.

Keywords: Service-oriented architecture, Enterprise security, Enterprise architecture, Security model

1. Introduction

In the past, two sides of a trade or transaction have been faced each other physically to exchange information or products. With time and human progress in various areas, this type of trade has been replaced with new methods. Development in advanced transportation systems, extensive postal networks and invention of telephone were including big changes that have transformed human life and gave it a new flavor.

When a phenomenon called personal computer came to the world and computer networks were also appeared followed by them, changes acceleration in human life took very fast upward. Today, the Internet and the Web become an integral part of life in the world and nobody denies the profound effects of these phenomenon on the life and customs of the people and their interactions and trading. The Web is now one of the most vital aspects of social life in modern societies: education, employment, government, management, information science, business, economics, policies, health, recreation, entertainments and various other aspects of social life are under the effect of the Web (Freire *et al* , 2008).

As mentioned, initial communications have changed to very complex procedures and each company and organization is trying to put itself ahead of the competition among other competitors. They are experiencing great changes and try to stabilize its position in the market for goods and services by using the latest technologies and methods. On the other hand, organizations made money just by buying and selling goods in past time and rarely offered services. But, today with the great changes were mentioned, some organizations are created only to provide services. These organizations offer a variety of services to other natural or legal customers from their facilities- which can be physical or other web services. This creates a new Internet concept called "Internet service". The services that are provided to the Web are called "web services"(23). Web service is not a new concept. It was existed in the past (Bell, 2008), but addressing it seriously is not more than 15 years.

In recent years, many concepts have entered into web service issue that has influenced almost all web domains. The appearance of technologies like XML, BPEL, etc. and protocols like SOAP, WSDL, UDDI and many contracts such as WS-Security, etc. change the concept of web services to a very broad concept (W3C, 2007, W3C, 2001, OASIS, 2004, Atkinson, 2002). With the expanding concept of web service, many companies and organizations were interested to use that. This technology makes it far less than the cost of a common information systems and let organizations to achieve higher earnings more than ever (Ibrahim and Miˇsi´c. 2006). With the widespread use of web services and extending to enterprise architecture, that the concept of service-oriented enterprise architecture have been made, some issues about the approaches are appeared for using this concept in a competitive manner. Security management in information systems was always one of the most basic and challenging issues that all companies have involved to it in using information systems (Korhonen *et at*, 2009). However, unfortunately this problem has not been considered as is worthy in many organizations except those have directly related to national defense and national or international security affairs. One of the reasons is that most of organizations are not familiar with the various aspects of this problem. This is true especially in information systems and information technology and networks in organizations. Service-oriented architecture is not exempt from this issue, especially when dealing with the concept of enterprise architecture combines and is going to serve as the organization's competitive advantage.

When a company wants to implement service-oriented enterprise architecture, one of the considerable issues is using a comprehensive and appropriate model (Valipour *et al*, 2009). In this research a new model for managing information security in service-oriented enterprise architecture is presented due to the growing interest for implementing service-oriented enterprise architecture in organizations and according to the need for creating an appropriate model for implementation.

This paper is organized as follow: part 2 will explain about choosing an appropriate basic framework for the proposed model, part 3 shows components, standards and models which have been affected the design of it. The proposed model is explained in part 4 and part 5 describes different components of the proposed model. Part 6 shows some result analysis, part 7 shows some results and finally a conclusion statement is explained in part 8.

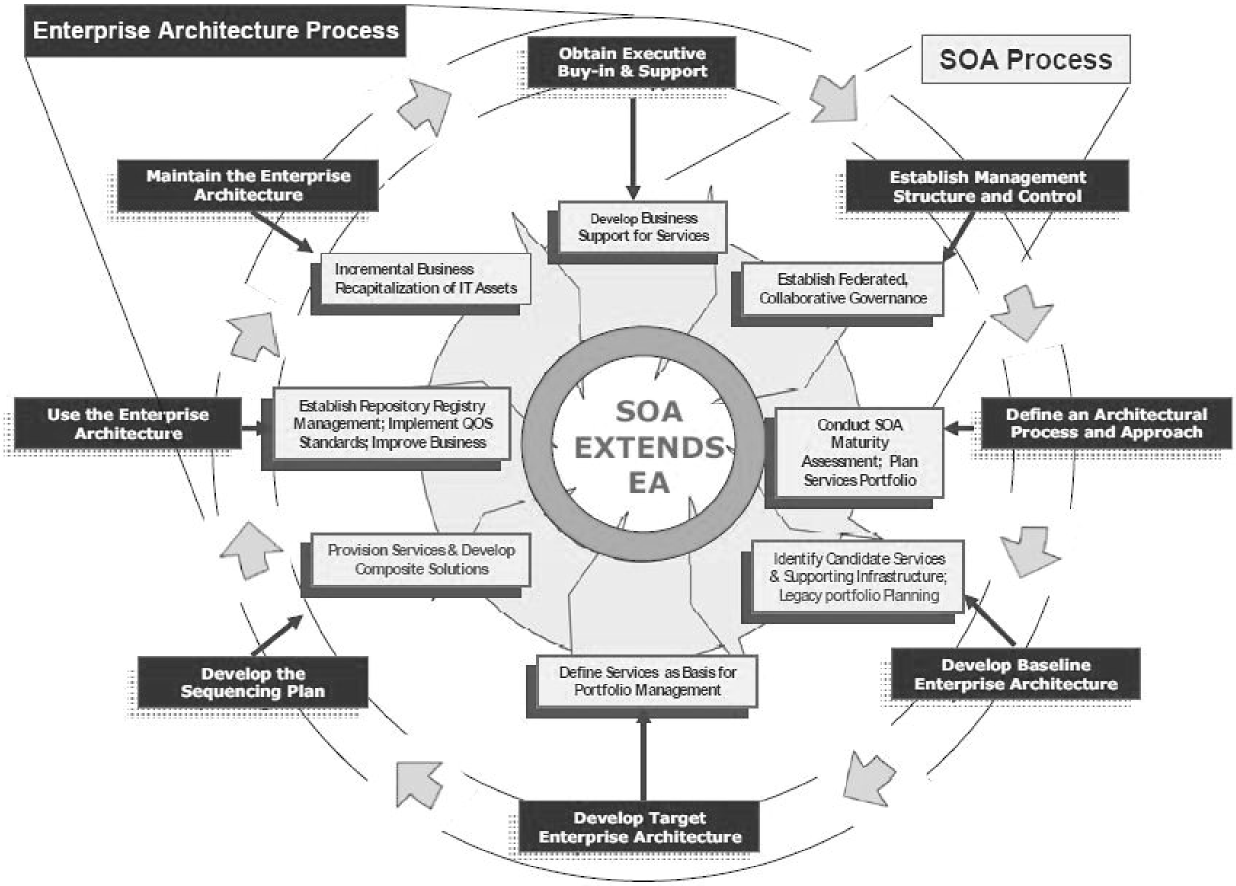
2. Choosing an Appropriate Basic Framework

One of the popular methods for designing a model is using existing architectures that are highly reputable and now are used in big companies and organizations. After various reviews on different reputable architectures and considering circumstances of such comprehensive model for enterprise architecture with extensive dimensions, finally, federal enterprise architecture framework (Roger sessions, 2007) has been selected as the foundation for the proposed model. However, significant changes have been applied on the final proposed model. Features that were influenced in the selection of federal enterprise architecture framework include:

1) The elements and components of enterprise architecture are well-defined in federal enterprise architecture framework (12).
2) Strategic goals and transition requirements are considered in addition to the products of different models of enterprise architecture.
3) There is no guidance on security and only some of the security issues surrounding infrastructure security had been mentioned in the service-oriented architecture version that was published in 2008(CIO Council, 2008)
4) The availability of federal enterprise architecture framework for service-oriented architecture guidance.
5) There is no definite prediction about transition plans

All above reasons led to chosen federal enterprise architecture framework (FEAF) as the foundation for the proposed model for information security management in comparison with other available frameworks. United States government published the latest version of federal enterprise architecture based on service-oriented concepts in 2008(CIO Council, 2008). Service-oriented lifecycle for federal enterprise architecture framework is shown in the following figure:

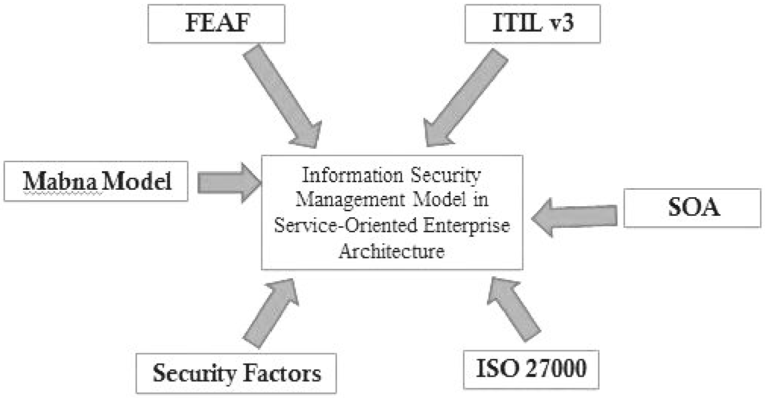
Figure 1: Service-Orientation lifecycle in federal enterprise architecture framework (CIO Council, 2008)


Enterprise Architecture Process
SOA Process
Obtain Executive Buy-in & Support
Maintain the Enterprise Architecture
Establish Management Structure and Control
Develop Business Support for Services
Incremental Business Recapitalization of IT Assets
Establish Federated, Collaborative Governance
Use the Enterprise Architecture
Establish Repository Registry Management; Implement QOS Standards; Improve Business
SOA EXTENDS EA
Conduct SOA Maturity Assessment; Plan Services Portfolio
Define an Architectural Process and Approach
Provision Services & Develop Composite Solutions
Identify Candidate Services & Supporting Infrastructure; Legacy portfolio Planning
Develop the Sequencing Plan
Define Services as Basis for Portfolio Management
Develop Baseline Enterprise Architecture
Develop Target Enterprise Architecture

3. Components, Standards and Models which have been Affect the Design of the Proposed Model

Various resources are used in designing the proposed model to achieve further characteristics of integrity, security and ease of implementation simultaneously. The following figure is shown these resources:

Figure 2: Standards, models and components that influenced on proposed model


FEAF
ITIL v3
Mabna Model
Information Security Management Model in Service-Oriented Enterprise Architecture
SOA
Security Factors
ISO 27000

- Federal Enterprise Architecture Framework: As mentioned above, FEAF is used as a foundation for designing the proposed model. Especially service-oriented guide for this framework that has been published in 2008 is considered.
- Service-Oriented Technology: Service-oriented architecture is one of the latest technologies for producing software and it seems to be used as the dominant architecture in the coming years (Newcomer and Lomow, 2005). This kind of software architecture uses software as services (SaS). In SaS model, software will be designed in a manner to be used in other systems and platforms (Erl, 2005). It means that everyone , who wants to use a service, should register and pay for that service. As mentioned, many standards and protocol like SOAP, WSDL, UDDI and some technologies like BPEL, XML, etc. are created to enrich service-oriented architecture.
- ISO 27000 Series Standards: ISO 27000 series standards are defined by Institute for Standardization Organization (ISO) for providing adequate information security domain. Among the members of the family include ISO 27001 that is related to information security management systems, ISO 27002 contains training for information security management implementation, ISO 2004 is related to measures for evaluating information security management, ISO 27005 is related to risk management in information security and etc..
- Mabna Model (Cyrus and Sabourtinat, 2010): Mabna model is a guidance for designing a practical strategic planning for implementing in organizations. Some parts of this model is used to identify information requirements, risk managements and developing security policies in the proposed model.
- Information Technology Infrastructure Library (ITIL v3.0) (Taylor *et al*, 2011): ITIL is a standard for IT management and include a series of successful experience and the best practices, patterns and methods in the area of information technology management that defines workflow process in an organization. ITIL is applicable to all organizations as a complete set of integrated software, hardware, workforce and network infrastructure, benefiting from organization experiences and practices, and the definition and concepts that is used in it don't depend on the organization type or structure. ITIL v3.0 is the latest version of ITIL. This version is based on service orientation concepts and each service is defined as work unit that contains different tasks.
- Security Factors (Avizienis *et al*, 2004): There are factors that have the greatest impact on information security management in service-oriented enterprise architecture. These factors are

very important and they are called "critical factors". Some of the most influential factors are listed below:

- Availability
- Integrity
- Confidentiality
- Reliability
- Reusability of services
- Authentication
- Authorization and access levels
- Non-repudiation
- Etc.

4. The Proposed Model for Information Security Management in Service-Oriented Enterprise Architecture

There are eight sections in federal enterprise architecture framework including (Shams and Mahjoorian, 2011):

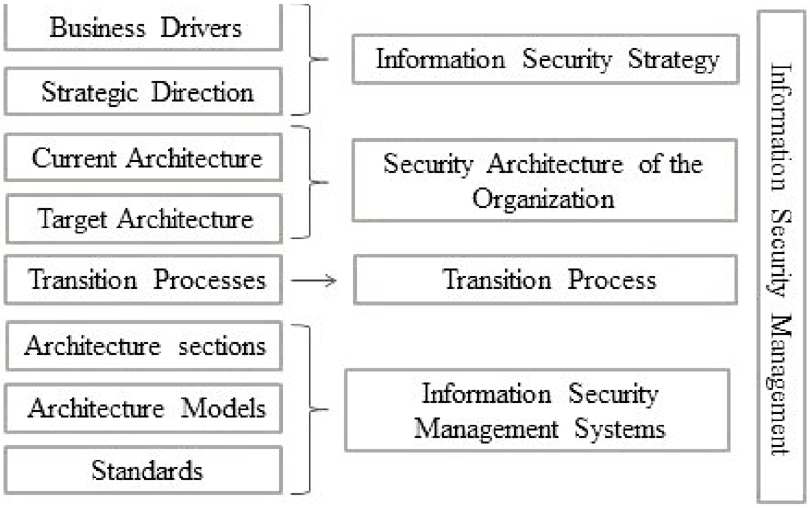
1) Business Drivers
2) Strategic Direction
3) Current Architecture
4) Target Architecture
5) Transition Processes
6) Architecture sections
7) Architecture Models
8) Standards

There are five sections in the proposed model for information security model that ensure efficiency in information security. These sections include;

1) Information Security Strategy
2) Security Architecture of the Organization
3) Transition Process
4) Information Security Management Systems
5) Information Security Management

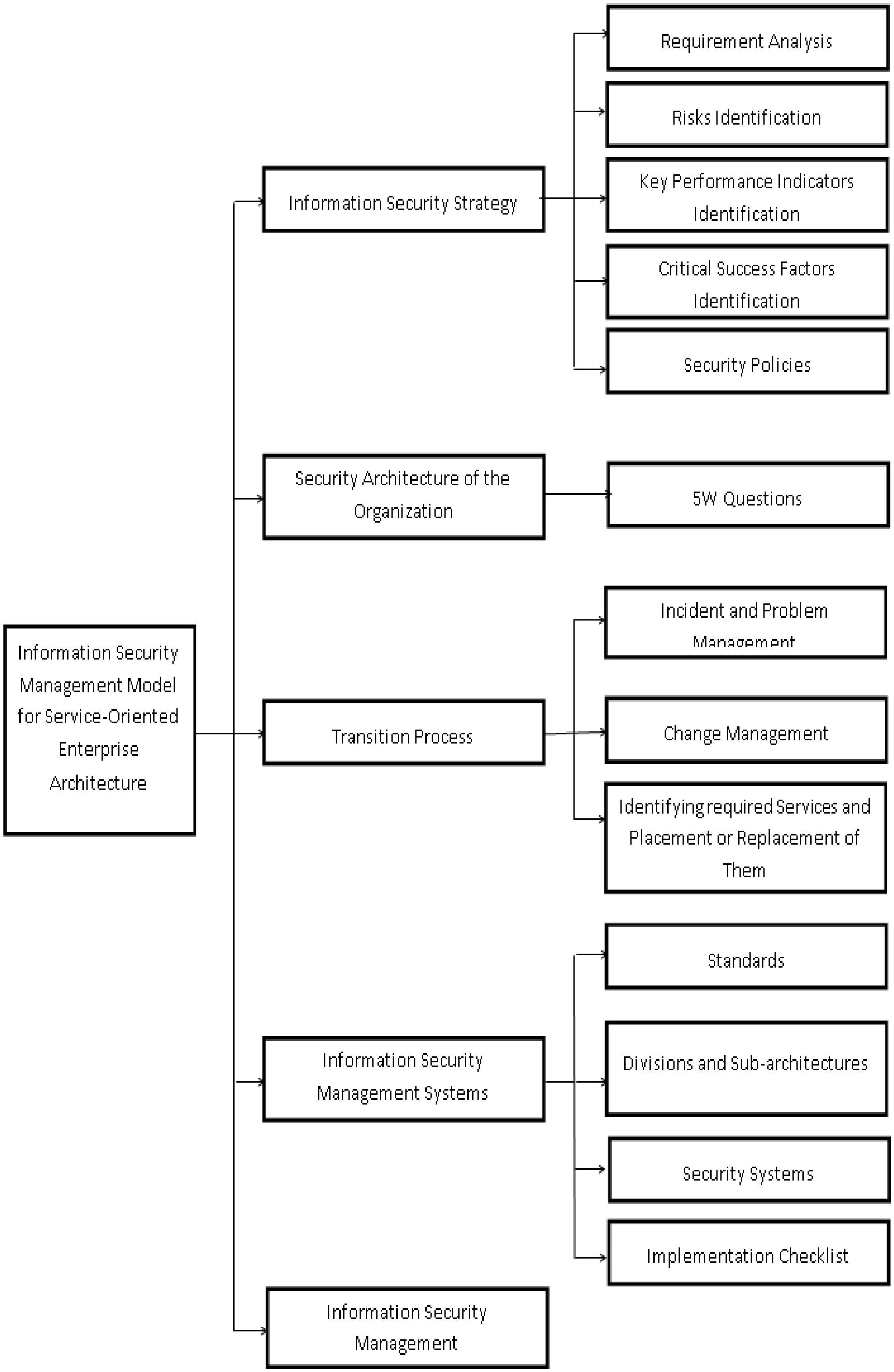
Mapping the sections of proposed model to sections of the federal enterprise architecture framework is shown in the following figure:

Figure 3: Mapping the FEAF parts to components of the proposed model



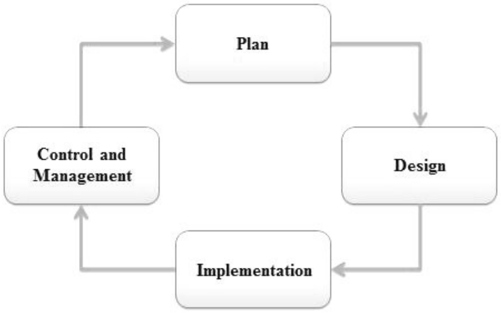
The proposed model is shown in the following figure:

Figure 4: The Proposed Model


Information Security Management Model for Service-Oriented Enterprise Architecture
Information Security Strategy
Requirement Analysis
Risks Identification
Key Performance Indicators Identification
Critical Success Factors Identification
Security Policies
Security Architecture of the Organization
5W Questions
Transition Process
Incident and Problem Management
Change Management
Identifying required Services and Placement or Replacement of Them
Information Security Management Systems
Standards
Divisions and Sub-architectures
Security Systems
Implementation Checklist
Information Security Management

There is a lifecycle for the model based on "Deming Cycle" that is used in each section of the model. This lifecycle is shown in the following figure:

Figure 5: Lifecycle in each part of the proposed model



It should be noted that in addition to considering how to solve security problems in the proposed model, there is a especial attention to avoiding security problems.

5. Components of the Proposed Model for Information Security Management in Service-Oriented Enterprise Architecture

In this section, the components of the proposed model will be explained:

5.1. Information Security Strategy

One of the main points that should be considered in enterprise security is the issue of strategy for the organization. Any models that have not considered strategy will be defeated. To achieve an appropriate strategy for an organization, following steps should be done**:**

a) *Security Requirements Identification*: This part specifies the requirements that organizations should consider to achieve the desired level of security to protect their information assets. These requirements include:

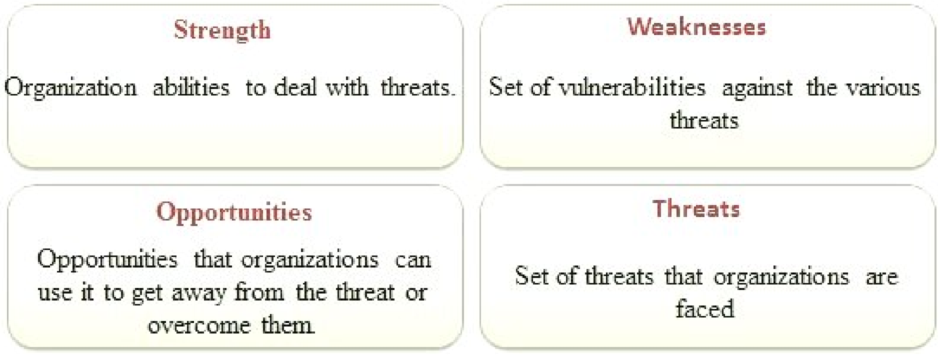
Table 1: Security requirements analysis factors

Internal requirements of organization	External requirements of organization
Organization's assets	Human resource requirements
Physical and environmental security requirements	Instrument security requirements
Information systems security requirement	Required controls
Report structures	Compatible with legal needs
Technical vulnerability management	Communication requirements
Information classification	Business continuity requirements
Data exchange	Governance factors

b) *Risks Identification*: Organization assets are usually threatened by risks. Risks can include threats or weaknesses that exist in an organization's information systems.
Risk= Vulnerability+ Threats+ Risk Probability+ Risk Impacts

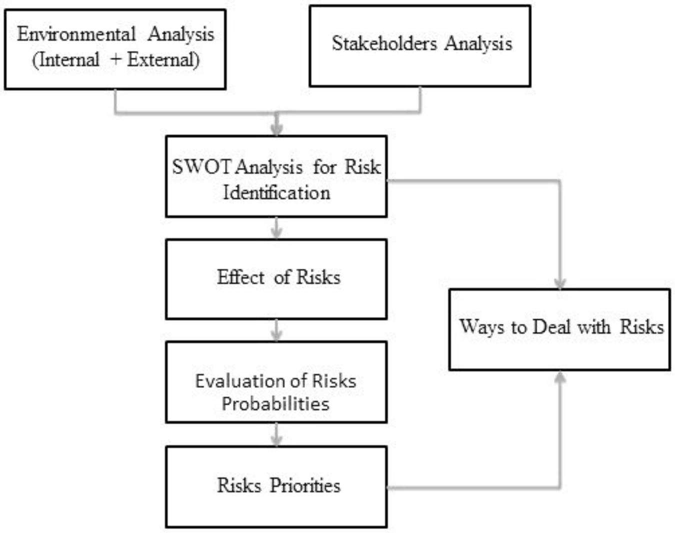
A kind of SWOT analysis (Strength, Weaknesses, Opportunities, Threat) is used in the proposed model.

Figure 6: SWOT analysis for risk identification


Strength
Organization abilities to deal with threats.
Weaknesses
Set of vulnerabilities against the various threats
Opportunities
Opportunities that organizations can use it to get away from the threat or overcome them.
Threats
Set of threats that organizations are faced

Before attempting to use SWOT analysis and prepare a list of the risks and solutions to deal with them, a careful review must be organized to identifying stakeholders and the environment that are associated with the organization. We should determine actual and potential risks. Procedures to identify and deal with risks are proposed as the following figure:

Figure 7: The proposed stages of identifying and dealing with risks in the proposed model


Environmental Analysis (Internal + External)
Stakeholders Analysis
SWOT Analysis for Risk Identification
Effect of Risks
Evaluation of Risks Probabilities
Risks Priorities
Ways to Deal with Risks

c) *Key Performance Indicators Identification*: Key performance indicator is directly related to the strategy and represents important information for organizations. KPIs are financial and non-financial measures that are used in determining the quality of the goals and reflect strategic performance of an organization. KPIs are used to evaluating current organization situation and specifying appropriate solutions for improving security. Identifiable indicators can be considered as potential candidates for KPIs. Some of these KPIs include:

- Reduction in the percentage of security in services.
- Reducing service downtime caused violation of safety factors.
- Increment in the acceptance and implementation of security procedures.
- Increment the support and commitment of senior management.
- Raise awareness about security policies and content access organization
- Etc.

d) *Security Critical Success Factors Identification*: Critical success factors are those factors that are vital for determining the success or failure of the business. Having these factors by the organization is a strategic and competitive advantage, and lack of them is a threat and strategic weakness for the organization. CSFs are factors that should be pre-determined to achieving goals. For analyzing critical success factors, any organization extracts various factors in accordance with its business activities.

e) *Security Policy*: Security policy determines who has what authorities to access which resources. The main purpose of a security policy is that users know what they are allowed to do. On the other hand, security policy can help system administrators and organization's managers to make decision about configuring and using the system. We can use other organizations experience to develop security policies or use helpful standards. Large and medium companies should follow a top-down approach for security policy, but small companies should follow a bottom-up approach. Every security policy defines the security goals of the organization and does not debate about engineering and implementation solutions. Security policy should be understandable, realistic and non-contradictory. It should be even economically feasible, practical, flexible, and fit to organization's goals. Security policy is composed of the following components:

- Statement about the policy
- How to apply the policy in the organization
- The role and responsibilities of the various people affected by the policy
- How flexible is the policy
- Legal and illegal activities and processes
- Rigidity and inflexibility of the policy

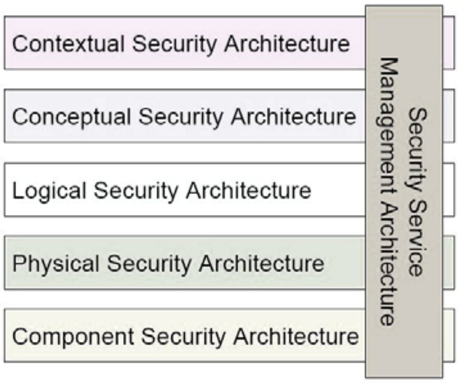
5.2. Security Architecture of the Organization

Security architecture of the service-oriented organization is a six layer model that has six views.

- Business view
- Architect's view
- Designer's view
- Builder's view
- Tradesman's view
- Service manager's view

This model is based on SABSA model (Sherwood *et al*, 2009) which is in the following figure:

Figure 8: Enterprise security architecture


Contextual Security Architecture
Conceptual Security Architecture
Logical Security Architecture
Physical Security Architecture
Component Security Architecture
Security Service Management Architecture

According to the above figure, each layer of the model is corresponding to one of the mentioned views. Contextual layer is corresponding to business view, conceptual layer is corresponding to architecture view, logical layer is corresponding to design view, physical security layer is corresponding to builder's view, component layer is corresponding to contractor's view, and security service manager layer is corresponding to service manager's view. Each layer of the security architecture model is defined based on 5W pattern (What, Why, Who, Where, When, How). The production of this model is shown in the following table:

Table 2: Enterprise security architecture products

	ASSETS (What)	**MOTIVATION (Why)**	**PROCESS (How)**	**PEOPLE (Who)**	**LOCATION (Where)**	**TIME (When)**
CONTEXTUAL ARCHITECURE	Business Decisions	Business Risk	Business Processes	Business Governance	Business Geography	Business Time Dependence
CONCEPTUAL ARCHITECTURE	Business Knowledge & Risk Strategy	Risk Management Objectives	Strategies for Process Assurance	Roles & Responsibilities	Domain Framework	Time Management Framework
LOGICAL ARCHITECTURE	Information Assets	Risk Management Policies	Process Maps & Services	Entity & Trust Framework	Domain Maps	Calendar & Timetable
PHYSICAL ARCHITECTURE	Data Assets	Risk Management Practices	Process Mechanisms	Human Interface	ICT Infrastructure	Processing Schedule
COMPONENT ARCHITECTURE	ICT Components	Risk Management Tools & Standards	Process Tools and Standards	Personnel Management Tools & Standards	Locator Tools & Standards	Step Timing & Sequencing Tools
SERVICE MANAGEMENT ARCHITECTURE	Service Delivery Management	Operational Risk Management	Process Delivery Management	Personnel Management	Management of Environment	Time & Performance Management

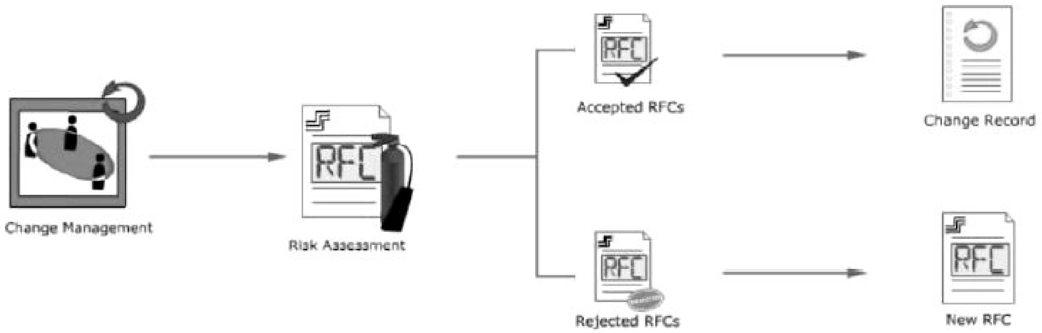
5.3. Transition Process

Transition process is one of the most important parts of an enterprise architecture that is used to transit from current architecture to the desired architecture. This process can not be considered as a separate and isolated process, but it is a process that has meaning in relation to other processes. Parts of this process include:

a) *Incident and Problem Management*: According to ITIL, incidents are events that commonly occur and there are specific solutions to overcome them. Various incidents and their solutions should be studied, predicted and documented in the security documents. On the other hand, problems are events that there is no predictable solution for them and show serious security problems and they should be resolved as soon as possible. After reviewing incidents and problems, it should be ensured that the predicted and used solutions don't cause further problems associated with other services. All incidents, problems and their solutions should be collected in a special database and this database should be updated constantly.

b) *Change Management*: Change management is one of the most important processes in ITIL. Any changes occur in the organization should passes through this process (Akram, 2005). This includes security issues too. Transition process is also a kind of change process. Therefore, measures must be devised to make the transition from old architecture to the new architecture don't disrupt business or downturn. For example, a change can be implemented step by step to reduce harmful impact of the new change on other parts of the organization. Another important point that should be considered is that any changes should be take place through a request for change (RFC). Requests are reviewed in a council called change advisory board (CAB). Change advisory board consist of IT professionals and senior managers of the organization and other managers to make decision about changes. The creation and adoption process of a request for change is shown in the following figure:

Figure 9: Create and adoption of RFCs



After approving the change, RFC will be sent to the technical department for implementation. In this stage, required tests will be done to minimize the harmful effects of changes on the business and services don't create security problems.

c) *Identifying required Services and Placement or Replacement of Them:* There are various methods for identifying required services:
   - Business process decomposition
   - Business functions
   - Business entity objects
   - Ownership and responsibility
   - Goal driven
   - Component based
   - Existing supply
   - Front-office application usage analysis
   - Infrastructure method
   - Non-functional requirements

5.4. Information Security Management Systems

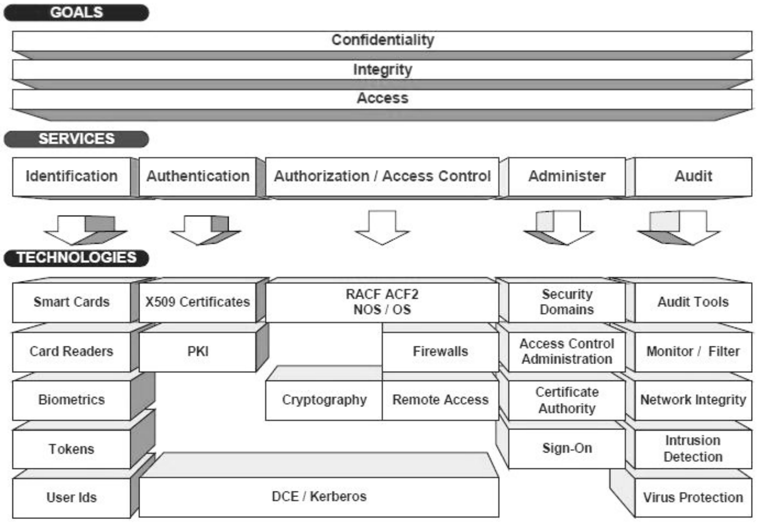
This section is more technical and provides a complete information security. Information security management systems are mechanisms that provide appropriate security guidelines to meet the requirements in the area of information security management. Among these mechanisms are:

a) *Standards*: Standards are comprehensive set of controls, including the best methods for evaluating the security of information and services and contain security details. The purpose of standards is that to be used as a resource to define a range of controls needed for most situations where information systems exist and they are used in business and industry. They essentially provide facilities to do business in a reliable environment. Usually different security information management standards are used in an organization simultaneously. Choosing appropriate standards for using in the organization depends on the type of the organization's architecture and information security management in it. Among widely used of information security standards are:
   - ISO/IEC 17799
   - BS 7799-2
   - ISO 27000

b) *Divisions and Sub-architectures*: For implementing the proposed model in the organization, it is better to divide processes and divisions into smaller parts and implement service-oriented architecture information security management factors on these parts. Then, extend the stages to upper levels. Generally, a bottom-up approach is recommended.

c) *Security Systems*: Security systems include technologies that must be considered in service security. However, this section is the most technological part of providing security for services. The relationship between technologies, services and business goals are shown in the following figure:

Figure 10: The relationship between security business technologies, services and goals



Considering the following items is essential for design and implementing services:

- Data Transition Security
- Message Security
- Application Security
- Data Security
- Knowledge Security
- Control Security

d) *Implementation Checklist*: A checklist that lists the steps for categorize and managing the resources, employer security, access controls and etc. can be useful for execute and maintaining activities.

5.5. Information Security Management

Main activities in this section are:

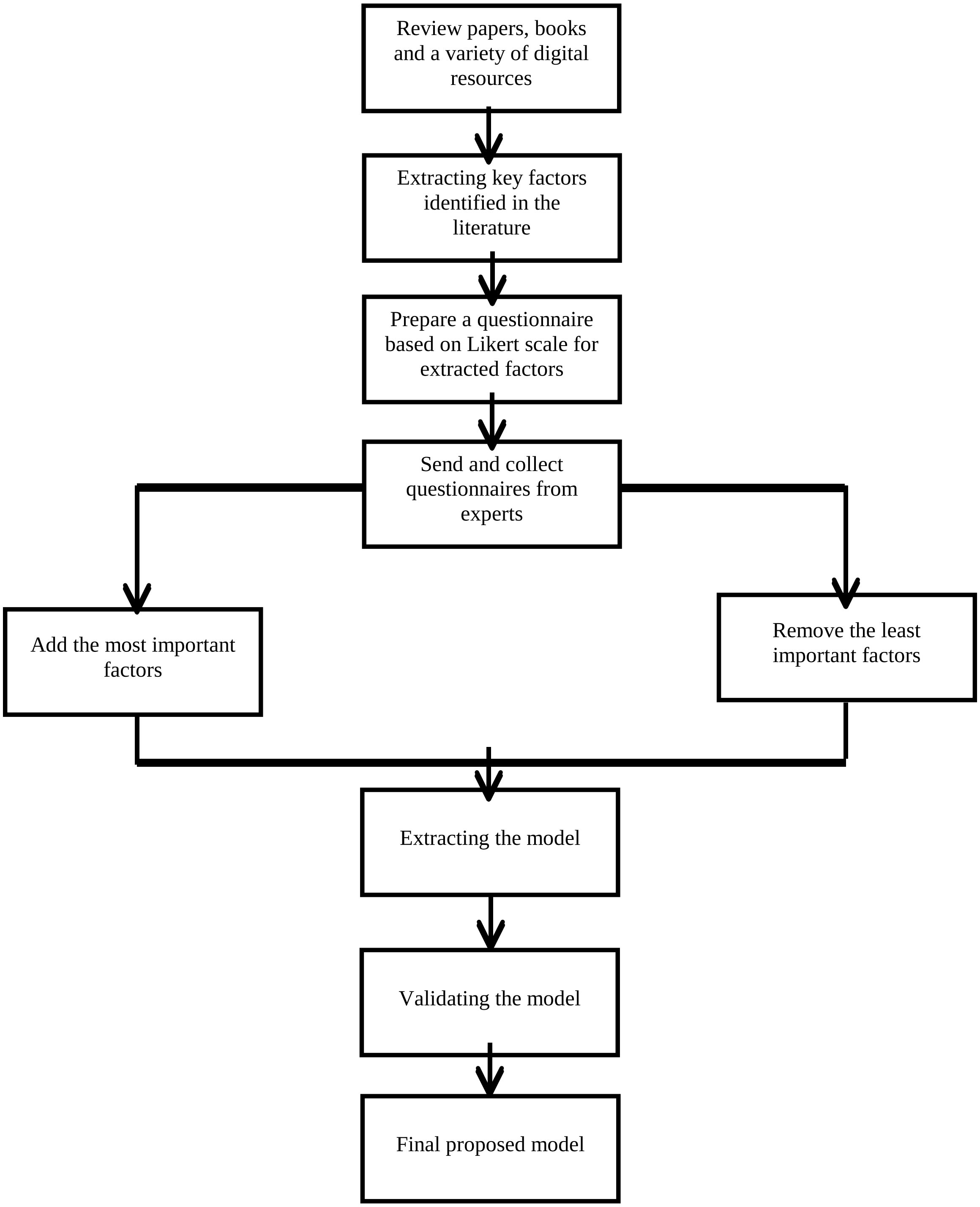
- Produce, review and amend all information security policies
- Implement and enforce security policies
- Evaluate and classification of documents and information
- Monitoring and handling all security incidents
- Analyze, report and reduce the impact of the risk
- Schedule and completion of security checking

This process monitors and reports all other components regularly and provides a variety of performance. All activities and tasks in other divisions of organization are recorded in a huge and integrated database in this section. The most important responsibility of this part is also creating a framework for managing information security management in an organization.

6. Discussion

In this research, a descriptive method was used. The method is based on questionnaire. The goal is collecting actual and wide variety of information from important factors of information security management in service-oriented enterprise architecture, and then, presenting a model based on the opinions of experts. To gather data for this study, various exploration methods have been used. These methods are classified in two categories: library methods (books, papers, digital contents) and non-library methods (questionnaire and interviews). The research workflow diagram is shown in the following figure.

Figure 11: The research process


Review papers, books and a variety of digital resources
Extracting key factors identified in the literature
Prepare a questionnaire based on Likert scale for extracted factors
Send and collect questionnaires from experts
Add the most important factors
Remove the least important factors
Extracting the model
Validating the model
Final proposed model

To determine the reliability of the questionnaire, Cronbach alpha coefficient was used. In this study the alpha was 82% that is a desired value.

As mentioned, the questionnaire was designed based on Likert scale (Oppenheim , 1996) (appendix A) . Here we show the average scores of experts answers in the following tables.

Table 3: The importance of essential security factors in service-oriented enterprise architecture

Factors	Confidentiality	Integrity	Availability	Authentication	Authorization	Trust	Non-repudiation	Utility	Ownership
Avg. score	4.42	4.54	4.26	3.96	4.18	3.87	4.06	3.84	4.32

Table 4: Quality of service values related to business quality

Factors	Service cost	Service suitability	Service aftereffect	Service brand value
Avg. score	4.26	4.64	4.12	4

Table 5: Quality of service values related to service level measurement quality

Factors	Performance	Stability
Avg. score	4.66	4.87

Table 6: Quality of service values related to suitability for standards

Factors	Conformability	Interoperability
Avg. score	4.20	3.96

Table 7: Quality of service values related to business process quality

Factors	Reliable Messaging	Transaction Processing Capability	Collaborability
Avg. score	4.42	4.32	4.86

Table 8: Quality of service values related to manageabiliy quality

Factors	Management Information Offerability	Observability	Controllability
Avg. score	4.44	3.82	4.26

Table 9: Critical success factors in the implementation of information security management in service-oriented enterprise architecture

Factors	Avg. score
Senior manager support	4.88
Improve communication processes with suppliers	4.24
Using best practice experiments	3.54
Training	3.72
Resource management	4.46
Proper technology	4.22
Plan a good strategy	3.86
Requirements analysis	4.62
Risk management	4.46
Security management	4.86

Table 10: The importance of service-orientation features in service-oriented enterprise architecture

Factors	Modularity	Loosely Coupled	Encapsulation	Reusability	Orchestration	Agility	Integrity	Self-Descriptive	Flexibility
Avg. score	4.12	4.56	4.32	4.74	3.94	4.2	4.63	3.78	4.72

7. Related Works

Many researches have been done on the issue of service-oriented architecture and many companies have presented different models. Among the more famous models are NASA security enhanced model for SOA (Pajevski, 2005), IBM service-oriented architecture security reference model (Nagaratnam *et al*, 2007), or concurrent technologies corporation (CTC) SOA security model (Youmans, 2009). Even great companies like Oracle, HP, Microsoft, etc. have their own solutions and security models for service-oriented architecture. But, there are less models about service-oriented enterprise architecture. Some researches worked on this issue. Among them are (Karimi, 2011, Tang *et al*, 2010, Sun and chen, 2008, Menzel *et al*, 2009, Bhallamudi and Tilley, 2011). Most of the introduced methods emphasize on technical views only. Some others emphasize on the business aspects more than technical aspects. So, it seems that a comprehensive model is needed for managing information security in service-oriented enterprise architecture.

8. Conclusion

Today, service-oriented technologies are popular all over the world. Organizations tried to take advantage of service-orientation in the competitive market. So, the idea of service-oriented enterprise came to the world. With the emergence of this idea, security challenges have been raised again as always. In this research, a new model for managing information security in service-oriented enterprise architecture has been presented. This model can help to IT managers, senior managers and everyone who wants to implement a secure architecture based on service-orientation in an organization or a company. The research method in this study is a descriptive method using questionnaires. Analyzing the opinions of experts who answered the questionnaire showed that the proposed model covers all aspects of an appropriate model for managing information security.

References

[1] Akram, M. S., 2005, "Managing Changes to Service Oriented Enterprises", Thesis submitted for Master of Science in Computer Science and Applications, Virginia Polytechnic Institute and State University

[2] Atkinson, B., 2002, "Web Service Security (WS-Security)", Available http://msdn.microsoft.com/en-us/library/ms951257

[3] Avizienis, A., and Laprie, J., and Randell, B., Landwehr, C., 2004, "Basic Concepts and Taxonomy of Dependable and Secure Computing", Technical Report 2004-47, Institute for systems research

[4] Bell, M., 2008, "Introduction to Service-Oriented Modeling", Wiley & Sons, ISBN 978- 0-470-14111-3

[5] Bhallamudi, P., Tilley, S., 2011, "SOA Migration Case Studies and Lessons Learned", IEEE International Systems Conference

[6] CIO Council, 2008, "A Practical Guide to Federal Service Oriented Architecture, Version 1.1", CIO, 2008

[7] Cyrus, K.M., Sabourtinat, A.H., 2010, "Mabna strategic management model", Tehran Polytechnic Press, Tehran, Iran

[8] Erl, T., 2005, "Service Oriented Architecture", Prentice Hall, PTR, USA

[9] FEA Consolidated Reference Model Document. at whitehouse.gov, 2007, "FEA Consolidated Reference Model Document Version 2.3', Executive office of the president of the united states

[10] Freire, A. P., Fortes, R. P., Turin, M. A., and Paiva, D. M. 2008, "An evaluation of web accessibility metrics based on their attributes". In proceeding of the 26th Annual ACM International Conference on Design of Communication (Lisbon, Portugal, September 22-24,2008). SIGDOC '08. ACM, New York, NY, 73-80

[11] Ibrahim, D., Miˇsi´c, V.B., 2006, "Service Views: a Coherent View Model of the SOA in the Enterprise", in Proceedings of International Conference on Services Computing, IEEE

[12] Karimi, O., 2011, "Security Model for Service-Oriented Architecture", Advanced Computing: An International Journal (ACIJ), Vol.2, No.4

[13] Korhonen, J. J., Yildiz, M., Mykkänen, J., 2009, "Governance of Information Security Elements in Service-Oriented Enterprise Architecture", in Proceedings of 10th International Symposium on Pervasive Systems, Algorithms, and Networks, IEEE, DOI 10.1109/I-SPAN.2009.158

[14] Menzel, M., Thomas, I., Meinel, C., 2009, "Security Requirements Specification in Service-oriented Business Process Management", International Conference on Availability, Reliability and Security

[15] Nagaratnam, N., Nadalin, A., Mostow, J., Muppidi, S., 2007, "SOA Security Reference Model", STSC CrossTalk, Available: http://www.stsc.hill.af.mil/crosstalk/2007/09/0709Nagaratnam NadalinMostowMuppidi.html

[16] Newcomer, E., Lomow, G., (2005), "Understanding SOA with Web Services", Pearson Education

[17] OASIS, 2004, UDDI Version 3.0.2, Available: http://uddi.org/pubs/ uddi_v3.htm

[18] Oppenheim, A.N., 1996, "Questionnaire design and attitude measurement", Heimann, London. Translated by Karimnia, M., published by Astan Ghods

[19] Pajevski, M., 2005, "A Security Model For Service-Oriented Architectures", NASA Web site: http://www.oasis- open.org/committees/download.php/17573/06-04-00008.000.pdf

[20] Roger sessions, 2007, "A comparison of the top four enterprise – Architecture Methodologies", msdn

[21] Shams, F., Mahjoorian, A., 2011, "The principles, fundaments and methods of service-oriented enterprise architecture", Shahid Beheshti University Press, Tehran, Iran

[22] Sherwood, J., Clark, A., Lynas, D., 2009, "Enterprise security architecture", SABSA Limited white papers, Available: www.learnSABSA.com

[23] "SOA Practitioners' Guide Part 3: Introduction to Services Lifecycle", 2006

[24] Sun, J., Chen, Y., 2008, "Intelligent Enterprise Information Security Architecture based on Service Oriented", International Seminar on Future Information Technology and Management Engineering, IEEE

[25] Tang, J., Dong, J., Zhao, Y., Tsai, W., 2010, "A Classification of Enterprise Service-Oriented Architecture", Fifth IEEE International Symposium on Service Oriented System Engineering

[26] Taylor, S., Lloyd, V., Rudd, C., 2011, "ITIL Version3", Best Management Practice

[27] Valipour, H., *et al*, 2009, "A Brief Survey of Software Architecture Concepts and Service Oriented Architecture", in Proceedings of 2nd IEEE International Conference on Computer Science and Information Technology, China

[28] W3C Recommendation, 2007, "SOAP Version 1.2 Part 1: Messaging Framework (Second Edition)", Available: http://www.w3.org/TR/soap12-part1/#intro

[29] W3C, 2001, "Web Services Description Language (WSDL) 1.1", Available: http://www.w3.org/TR/wsdl

[30] Youmans, J., 2009, "Methods of SOA Security Engineering and Certification", Concurrent Technologies Corporation Web site: http://www.jeff-youmans.com/PPT/Youmans%20DoDIIS %20WorldWide%2008.ppt

Appendix A

1) Do you think it's a good strategy to insulate the direct contact between service consumer and service provider?

Yes □
No □
Because ………………………………………………………………………………

2) Please rank the level of importance of security requisites in service-oriented enterprise architecture.

(5=very important, 4=important, 3=medium, 2=less important, 1= not important)

Requisite	**5**	**4**	**3**	**2**	**1**
Confidentiality Integrity Availability Authentication Authorization Insurance Trust Non-Repudiation Responsibility Utility Possession					

3) To what extent do the following quality of service aspects address the service-oriented enterprise architecture security?

(5=very important, 4=important, 3=medium, 2=less important, 1= not important)

Factors		**5**	**4**	**3**	**2**	**1**
1	Business Value Quality Service cost Service suitability Service Aftereffect Service Brand Value					
2 3	Service Level Measurement Quality Performance Stability Suitability for Standards Conformability Interoperability					
4	Business Process Quality Reliable Messaging Transaction Processing Capability Collaborability					
5	Manageability Quality Management Information Offerability Observability Controllability					
6	Security Quality Confidentiality Integrity Authentication Access Control Non-Repudiation Availability Traceability Privacy Distributed Authorization					

4) To what extent do the following items influence in successful service-oriented enterprise architecture security implementation?

(5=very important, 4=important, 3=medium, 2=less important, 1= not important)

Factor	5	4	3	2	1
Senior manager support Improve communication processes with suppliers Using best practice experiments Training Resource management Proper technology Plan a good strategy Requirements analysis Risk management Security management					

5) Please rank the level of importance of service-oriented specifications in service-oriented enterprise architecture security.

(5=very important, 4=important, 3=medium, 2=less important, 1= not important)

Specification	5	4	3	2	1
Modularity Loosely Coupled Encapsulation Reusability Orchestration Choreography Agility Framework Independency Self-Descriptive Integrity Flexibility Gradual Development Affordability					

6) To what extent are the following approaches relevant the characteristics of an architecture that addresses the use of security?

(5=very important, 4=important, 3=medium, 2=less important, 1= not important)

Style	Description	Rank
Enterprise web service approach	It is SOAP-based enterprise service architectural style. Specifically the style is based on a series of web service standards.	
Enterprise web-oriented architecture	The Web SOA (WOA) based on REST architectural style and enterprise Web 2.0 is another substyle of the ESOA	
Enterprise event-driven architecture	It is Enterprise Event-Driven Architectural style which is a hybrid style with ESOA	
Enterprise component-based service architecture	It is Enterprise Component-Based Service Architectural style which is based on service component-based specifications, such as SCA.	
Enterprise grid-enabled service architecture	It is Enterprise Grid-Enabled Service Architectural style which is a hybrid style with ESOA and Grid computing style.	

Other………………………………………………………………………………………

7) According to your experiences are any of proposed requisites of service-oriented specifications (loosely coupled, agility, integrity, etc.) in conflict with others? Please write down these issues.

…………………………………………………………………………………………………
…………………………………………………………………………………………………
…………………………………………………………………………………………………
…………………………………………………………………………………………………
…………………………………………………………………………………………………

8) According to your opinion, what are three most crucial service-oriented supply chain management metrics?

1)………………………………………………………………………………………………

2)………………………………………………………………………………………………

3)………………………………………………………………………………………………