UNIVERSITY OF GOTHENBURG

An Integrated Security Model for the Management of SOA

Improving the attractiveness of SOA Environments through a strong Architectural Integrity

VIVEK JONNAGANTI

Master Thesis work in Software Engineering and Management

Report No. 2009-055
ISSN: 1651-4769

University of Gothenburg
Department of Applied Information Technology
Gothenburg, Sweden, May 2009

Abstract

The main purpose of this thesis is to create an integrated model for an attractive, collaborative and secure environment shaped by Service-oriented Architecture (SOA). In order to create and verify the proposed model the managerial and governance aspects of SOA requisites were also considered. The proposed model has been created to provide a sound response to the following enquiry: "What concepts and principles should define a secure collaborative and attractive service environment?" In order to provide a more fruitful answer the above query was decomposed into three corresponding questions namely; (1) Why is security such a crucial issue for a service environment?, (2) How can the security of a collaborative service environment improved trough the application of Confidentiality, Integrity, and Availability (CIA) concept? (3) Are the principles and concepts of CIA triad enough, or must they be updated first and then integrated to the SOA concept as well as to the enterprise of SOA Governance? Accordingly this work concludes the following;

Firstly, in many cases a SOA environment can be neither attractive nor collaborative if the aspects of security are excluded from the architecture. Therefore this study provides an extended model of SOA where the providers of such an environment should never be directly accessed by consumers. This requisite implies a modified configuration that shapes a SOA environment.

Secondly, the proposed model is the result expected by the requisites for integrating SOA and CIA principles. Accordingly an attractive, collaborative environment must be designed and maintained with respect to its foundational principles. In other words, such an environment must always demonstrate its agreement with the foundational principles.

Lastly, the proposed model extends the primary requisites of security such as Confidentiality, Integrity and Availability to include even requisites such as Authorization, Authentication, Identity, Auditing, Compliance and Security Policies. By this way the proposed model provides a more complete foundation for a secure SOA environment.

In summary, the proposed model promotes the architectural integrity of SOA as we have eliminated principles that do not belong to SOA. Instead, we have added principles of security to the foundational principles of SOA. The proposed model is based on the existing concepts and principles of SOA as well as CIA. The reusability principle has to be excluded from the concept of SOA because this principle creates contradictory results and unnecessary interdependencies. Lastly, the environment we refer to is an attractive and collaborative service environment aiming to response to all requisites of enterprise Agility. This study has been designed and implemented through the creation, validation and verification of the proposed model. Accordingly, the model demonstrates an excellent correspondence between the theoretical and empirical views covered by the study. However, due to the few underlined interviews some form of generalization cannot be provided.

Keywords: Service-oriented Architecture (SOA), Confidentiality Integrity Availability (CIA), Additional security principles, Proxy Services, Extended SOA Governance.

Supervisor: Dr. Thanos Magoulas.

Acknowledgements

The writing of this thesis has been one of the most significant academic challenges that I have undertaken till date. I would like to thank my academic supervisor Dr. Thanos Magoulas for his diligent support, patience and guidance throughout the duration of my work. This work would not have been possible without his support.

I would also like to thank all the respondents who took part in the empirical study and gave me interesting insights into the subject.

Lastly, I would like to thank my friends and family for their encouragement and support.

Vivek Jonnaganti
May 2009,
Gothenburg.

Table of Contents

List of Figures

1. Introduction

This section provides an introductory understanding of Service-Oriented Architecture (SOA) and its relation to the CIA security triad (Confidentiality, Integrity and Availability). It also provides the reader an insight of the security issues that must be satisfied by SOA. The purpose, problem statement and delineation of the study are defined, along with an outline for the process of inquiry. Lastly, the different parts that together form the report are outlined.

1.1 Background

1.1.1 The Swedish Tax Agency and the LIBRIS Environment: Service Oriented and Architected Environments

We would like to start this study by stating two real cases of service environments and their necessary requisites for security. A secure service environment is not sufficient but necessary to satisfy the requisites of an attractive and collaborative environment.

On January 2004, the Swedish National Tax Board and ten other regional tax authorities were merged into a nationwide agency, called the Swedish Tax Agency (Regeringskansli, 2009). This Agency is responsible for the operational aspects of taxation. The Agency's head office located in Solna, ensures that the tax rules are applied consistently by issuing regulations and providing general advice and training. The main tasks of the Swedish Tax Agency are processing income statements, income tax returns on an annual basis, and processing corporate tax returns on a monthly basis.

According to the Government website, every year companies send in specifications on salaries paid and tax withheld in the form of income statements for employees. Banks send in income statements on interest and similar matters, and insurance companies send in income statements on premiums paid on pension insurance schemes. This extensive obligation for employers, banks and insurance companies to submit income statements has made it possible to send out pre-printed tax returns. If the pre-printed information is complete and accurate, the person filing the tax return can simply sign it and mail it to the Tax Agency. It is also possible to file the tax return electronically via the Internet or by using the telephone or text messaging. In 2006, some 2.6 million persons used this option to file their tax returns.

LIBRIS is the National Union Catalogue of Sweden, making available bibliographic services such as search, cataloguing and inter-library lending. LIBRIS provides public access to over seven million titles in over 190 Swedish libraries (Larsson, 1998). The titles represented are books and periodicals, as well as journal articles, maps, printed music, posters and electronic resources. About 200 libraries from the other Nordic countries use LIBRIS for inter-library loans (LIBRIS, 2009). These libraries include academic, research as well as public libraries. LIBRIS does also comprise a variety of sub-databases within different areas, national bibliography, subject specialized, local/regional etc.

This system makes use of the Service-oriented Architecture (SOA), where LIBRIS acts as the service broker and helps various libraries acting as service providers to collaborate and exchange information with the service consumers i.e. students, lecturers and researchers (Kingkarn, 2008). The Swedish Tax Agency also makes use of this architecture, where the Agency's Head Office and the regional tax authorities intermittently act as service brokers helping employers, banks, and insurance companies to notify income statements. Similarly, they also help tax payers to file returns using various communication channels.

One of the key challenges of the architectures discussed above is providing the appropriate levels of security. The different entities of the architecture i.e. service broker, service consumers and service providers communicate on an ad-hoc basis (as and when the need arises). Security models built into a specific entity may no longer be appropriate, when the capabilities of these entities are exposed as services that can be used by other entities.

For some businesses such as the Swedish Tax Agency, security is extremely vital and critical. Security is also considered as a pre-condition in business areas such as banking, healthcare, industrial research, e-commerce etc. It is clearly the fact that security is a business requirement, not just a technical attribute. Any security approach adopted should be in alignment with the architectural integrity of SOA.

1.1.2 Understanding the idea of a Service-Oriented Architecture

Service-Oriented Architecture (SOA) is a method underlying systems development and integration where system functions are grouped around business processes and are packaged as interoperable services[1] (Wikipedia, 2009). According to Josuttis (2007), SOA is not a concrete tool or a framework but rather an approach, a paradigm that leads to certain concrete decisions when designing concrete software architecture. Finally, OASIS[2] defines SOA as "a paradigm for organizing and utilizing distributed capabilities that may be under the control of different ownership domains. It provides a uniform means to offer, discover, interact with and use capabilities to produce desired effects consistent with measurable preconditions and expectations."

Technically, SOA can be defined in terms of relationships between (1) A domain of Service Consumers, (2) A domain of Service Providers and, (3) A domain of Service Brokers[3] (Kingkarn,

[1] A service is a unit of work done by a service provider to achieve desired end results for a service consumer. Both provider and consumer are roles played by software agents on behalf of their owners (Hao 2003).

[2] The Organization for the Advancement of Structured Information Standards (OASIS) is a global consortium that drives the development, convergence and adoption of e-business and web service standards (Source: Wikipedia)

[3] A service broker is neither a consumer nor a provider but a third part that is necessary where a service or business process is composed of several more elementary services that belong to different owners. In this sense, a broker provides information of what services are provided by whom (Kingkarn 2008).

2008). These three domains form together a so-called Service-based Business Environment (see Figure 1).

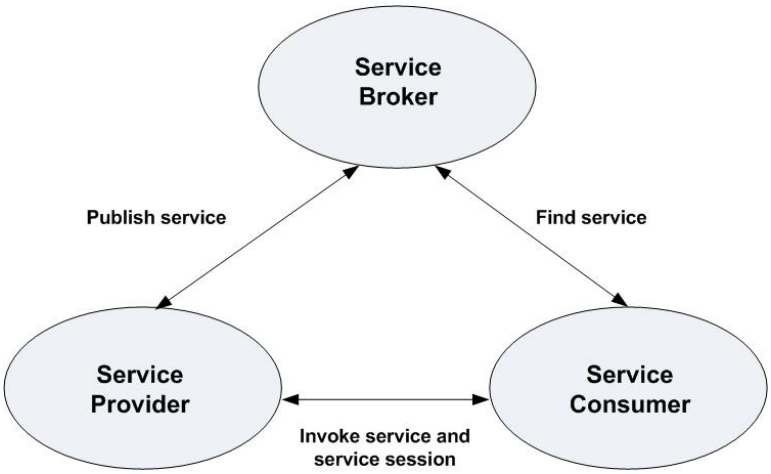


Figure 1 - Service based business environment (Kingkarn 2008)

1.1.3 SOA Security; An Issue of Confidentiality, Integrity and Availability?

Confidentiality, Integrity and Availability (CIA), is a widely used benchmark for evaluation of information systems security. For over many years, information security has held that CIA, also known as the CIA triad (see Figure 2) as the core principles of information security. The Generally Accepted System Security Principles[4] (GASSP) defines information security principles in a broad context. It includes principles, standards, conventions and mechanisms (GASSP, 1999). GAASP terms CIA as pervasive in nature and fundamental to all information systems.

Another organization, the National Institute of Standards and Technology[5] (NIST) defines computer security as "the protection afforded to an automated information system in order to attain the applicable objectives of preserving the integrity, availability, and confidentiality of information system resources." These principles apply irrespective of the technology platform (hardware, software or firmware), communication channels, size of the organization etc. According to NIST, the three tenets for which security practices are measured can be described as follows;

[4] The key objective of the GASSP community is to identify and develop pervasive, broad, functional and detailed security and protection profiles in a comprehensive framework of emergent principles which helps to preserve the confidentiality, integrity and availability of information.

[5] NIST is a measurement standards laboratory which is a non-regulatory agency of the United States Department of Commerce. The institute's mission is to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve quality of life (Source: Wikipedia).

- **Confidentiality:** A requirement that private or confidential information not be disclosed to unauthorized individuals.

- **Integrity:** Data integrity is a requirement that information and programs are changed only in a specified and authorized manner. System integrity and Application integrity are requirements that a system or application performs its intended functions in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation.

- **Availability:** An assurance that a system works promptly and service is not denied to the authorized users.

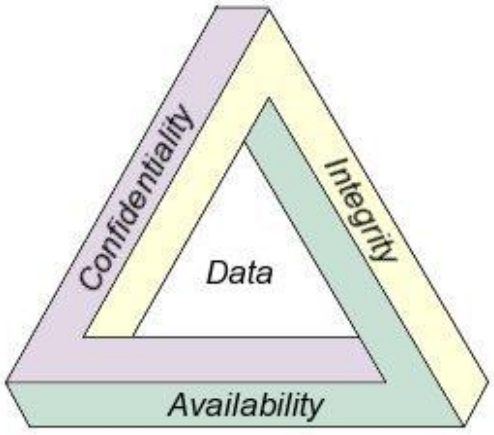


Figure 2 - CIA Triad

However, these crucial aspects of security despite their necessity are not sufficient for the creation of a secure SOA environment. Therefore, this study has tried to identify all those factors that – at least in theory – are concerned as relevant and important for the creation and maintenance of a secure SOA Environment. Later on in this study, we shall present the extended model of SOA and SOA Governance with respect to the issues of CIA.

1.1.4 Need for SOA security

The functioning of SOA requires the service consumer to be able to connect to the service broker (find service) and subsequently the service provider (invoke service). Similarly, the service provider has to be able to connect to the service broker (publish service) and the service consumer (provide service). This implies that there is an imperative for all service domains to connect to each other without any considerations of security and trust. In case of the traditional client server architecture, the server application is assumed to be aware of the appropriate security model and also responsible for decisions regarding security. Henceforth, the server application is trustworthy to monitor all the data including sensitive information that the client is sending. The increased exposure of services in SOA brings a greater potential for compromise as each service becomes a vulnerable attack point (Pajevski, 2004). At the same time, greater damage is inflicted due to the increased exposure of data which needs to be protected at both transit and rest.

In the case of SOA, an application can be composed of services from multiple applications. A service can be invoked in different contexts by different client applications, which means it can never tell how it should handle security. Applications alone can no longer be in charge of security and security models cannot be hard-coded into applications (Ramarao & Prasad, 2008). Another issue is that some or all parts of a message intended for one enterprise's application may end up with another application. So it's important to have some mechanism to limit the data exposed to each application. In other words, as application and enterprise boundaries are no longer impediments to reuse, traditional approaches to security no longer suffice (Ramarao & Prasad, 2008). Also, the success of SOA implies on the transmission of large volumes of real-time business critical information which makes it more vulnerable to security threats.

Security infrastructure should be accessible independent of technology, using open standards. A number of new technologies and standards are emerging to provide more appropriate models for security in SOA. A critique of these standards is that they delve in solving the problem of security in the implementation stages rather than focusing on the design aspects. It is henceforth essential to consider the impediments to security from an architectural perspective and solve the issue of security using a holistic approach.

1.2 Purpose of the study

The main purpose of this thesis is to create an integrated model which defines a secure, attractive and collaborative SOA-environment. The integrated model will be obtained by extending the principles of the CIA triad and then to integrate them with the principles and requisites of SOA. A better understanding of security in terms of SOA and CIA will provide a better platform for specifying requisites to be satisfied by any technical solution.

The integrated model will be checked for completeness and consistency i.e. conformance to the problem domain by making use of a proven research methodology. Also, in order to create and verify this model the managerial and governance aspects of SOA also needs to be considered as they play pivotal roles in shaping the SOA business environment.

1.3 The problem statement of the study

In accordance to the purpose of the study stated above, the problem statement can be stated as follows;

What concepts and principles should define a secure, collaborative and attractive service environment?

The CIA triad is a widely used information assurance[6] (IA) model that identifies the fundamental security characteristics of all information systems. However, in order to provide a fruitful solution the above problem statement can be decomposed to provide the basis for an explanatory theory that promotes the understanding of the following issues;

- Why is security such a crucial issue for the service environment?
- How can the security of a collaborative service environment improved trough the application of CIA[7] concept?
- Are the principles and concepts of CIA triad enough, or must they be updated first and then integrated to the SOA concept as well as to the enterprise of SOA Governance?

1.4 Delineation of the study

This study focuses on environments consisting of consumers, providers and brokers. A Service Oriented Architecture is expected to integrate loosely all involved parties and create a collaborative attractive environment e.g. LIBRIS.

The study focuses on devising comprehensive integrated security model rather than focusing on specific security issues. At the same time, specific security issues can be tackled using the integrated model as it provides a holistic approach to deal with security. The integrated security model will be tested, verified and evaluated empirically.

SOA Services are sometimes equated with Web-services. However, SOA Models defines the problem whilst Web-services belong to the solution space (one of the alternatives) for implementing the ideas of SOA. SOA is an enterprise model that is implemented by both human and non-human resources. The issues of SOA implementation are not considered for this study.

1.5 Outline of the inquiry process

The approach of the inquiry process for this study consists of the following stages. Firstly, the creation of a conceptual framework (the theory underlying in this study) derived from the primary problem statement of the study. Secondly, the creation of a security solution derived from the distillation of theoretical ideas and models regarding SOA security. Similarly, empirical views will help us to attain the attitudes and perceptions of people concerning both the characteristics of SOA and SOA Security. Lastly we present a discussion, by deriving similarities and differences between

[6] Information assurance (IA) is the practice of managing information-related risks. More specifically, IA practitioners seek to protect and defend information and information systems by ensuring confidentiality, integrity, authentication, availability, and non-repudiation (Source: Wikipedia).

[7] The concept of CIA (Confidentiality, Integrity and Availability) implies to the reality of information bases, information flows and information processing that takes place in our business or public environment.

the theoretical and empirical views of SOA security with respect the various issues of SOA, CIA and SOA Governance.

1.6 Outline of the report structure

The rest of the thesis is divided into six chapters as illustrated below (see Figure 3). In chapter 2, we describe the methodology followed in this thesis followed by the model delineation and scoping. Chapter 3 deals with the theoretical views of a SOA originated environment with respect to CIA. The security requirements of a SOA architected environment is discussed in this chapter. In chapter 4, we describe the nature of empirical inquiry and queries for the validation of the SOA security model.

In chapter 5, the findings of the empirical study are analyzed in relation to the theory i.e. the goodness of the proposed model is verified. Chapter 6 deals with the discussion where the theoretical and empirical views are compared. At the end, we conclude the thesis and summarize the contribution made by this research.

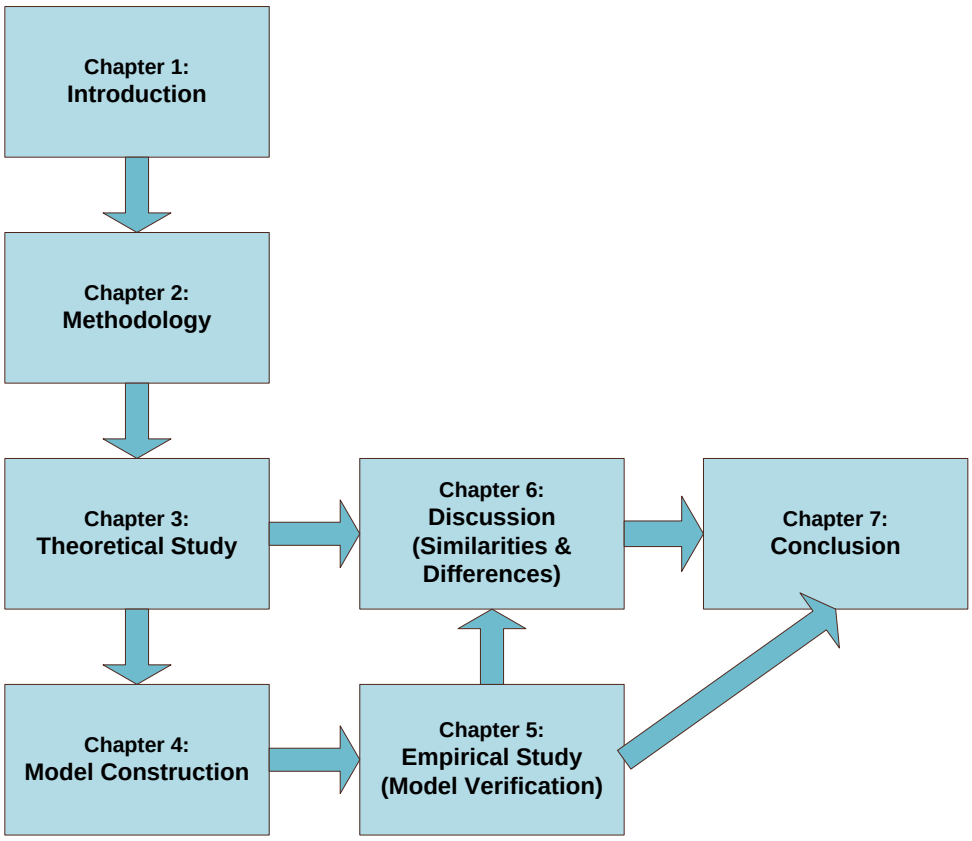


Figure 3 – Outline of the report structure

2. Methodology

In this section, we describe the methodology employed in this study. The approach that has been followed in understanding the security aspects of SOA are both normative (theory driven) and descriptive (experience driven). The purpose of the chapter is to explain the need and choice of following a particular methodology and also to present the methodology followed in this thesis.

2.1 Establishing the foundation underlying the proposed solution

The main concern of this thesis is to develop an integrated security model that promotes the choice of a comprehensive architectural pattern, as well as explain how the proposed architectural pattern promotes security of the service-based business environment. To achieve this we will need to understand the security requirements and challenges encountered to implement a security solution for the service-based business environment. It is also important to offset this study by understanding the existing security models, as this could be compared with the proposed model.

The concept and principles of the CIA triad have to be understood and evaluated, in order to determine its strengths and weakness. An extended idea of security can be ascertained by deriving old and new security concepts and principles. Finally, this extended idea of security should be integrated with the concepts and principles of SOA.

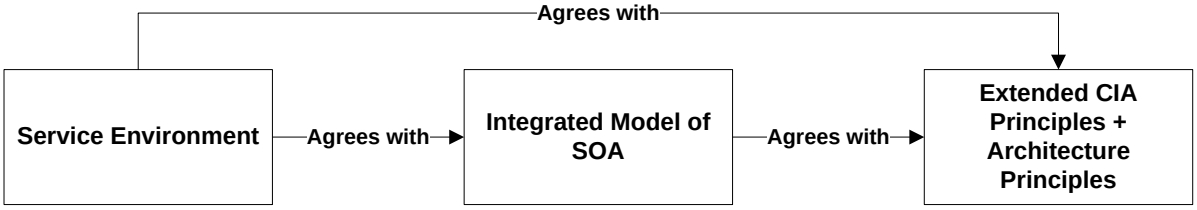


Figure 4 – Towards a sound theory of SOA Security

As we can see in Figure 4 above, the logical nature of the inquiry can be expressed in the following way;

- Demonstrate that the service environment agrees with SOA.
- Demonstrate theoretically that SOA agrees with the extended principles of CIA and architectural principles.

Henceforth, demonstrate that the service environment agrees with the extended principles of CIA. The demonstration of these inquiries should provide the answer to our thesis. This hypothesis is derived from the theory of Nicholas Rescher who states that knowledge is a system of principles. Reality agrees with knowledge and hence reality agrees with a system of principles (Rescher, 1979).

It has to be demonstrated both theoretically and empirically that such an integrated concept can define a secure, attractive and collaborative environment (see figure 5). In other words, SOA should provide the conceptual means upon which the real collaborative environment should be conceived and evaluated as attractive. At the same time, the extended CIA model should provide the conceptual means upon which the same real collaborative environment should be evaluated and conceived as secure. The completeness and delineation of the model are to be determined by formulating questions which are in conformity to the purpose of this study.

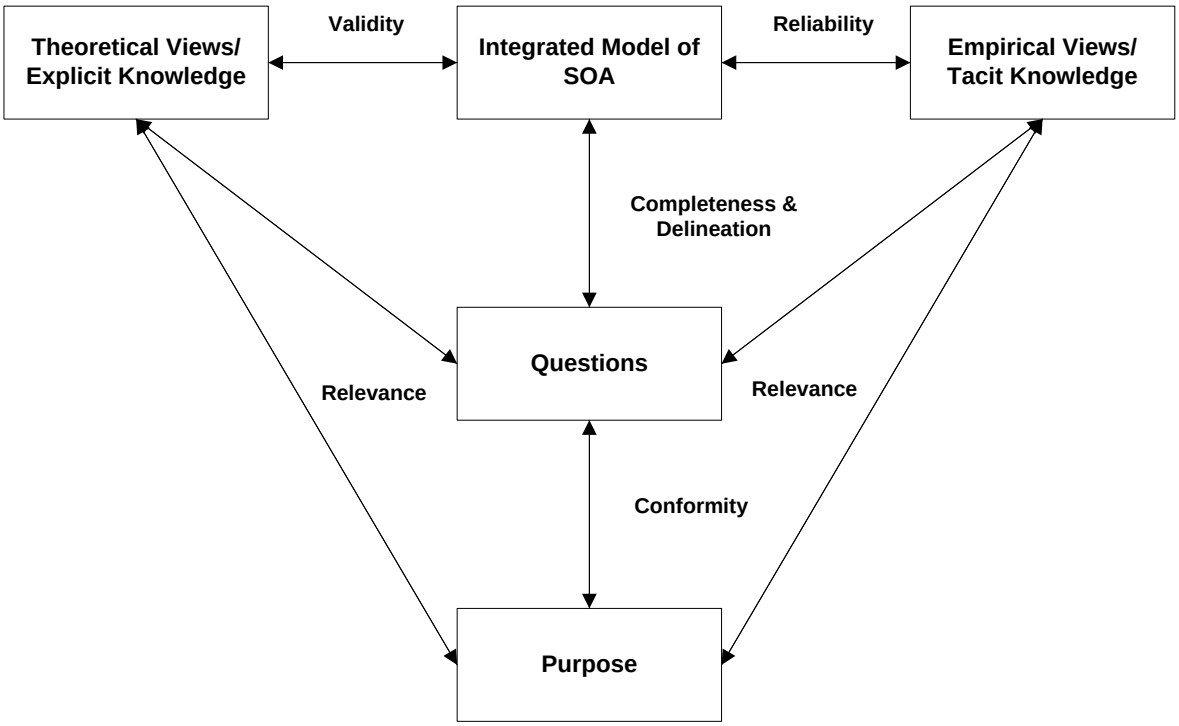


Figure 5 – Thesis Methodology

2.2 Model delineation and scoping

The first step in the inquiry process is to understand the complexity of the SOA architectures. We already know that the concept of SOA is based an architectural style that defines an interaction model between three primary parties (Arsanjani, 2004);

- The service provider, which publishes a service description and provides the implementation for the service.
- A service consumer, which can use the service description directly of find the service description in a service registry.
- The service broker provides and maintains the service registry.

A meta-model is depicted in the figure below (see figure 6). The primary variation in this architectural style is with respect to the use of the service broker i.e. the consumer can directly obtain the service description from the provider instead of using the broker, which implies that the broker is an optional component. However, both these architectural variations exist and are exploited as per the system requirements. In order to device a comprehensive and integrated security model we have to consider an architecture which includes the broker. The possibility of having a specialized broker presents many challenges with respect to the security requirements and system design. Therefore, moving forward for all practical purposes we shall consider SOA architecture with consumers and providers with the presence of an explicit broker.

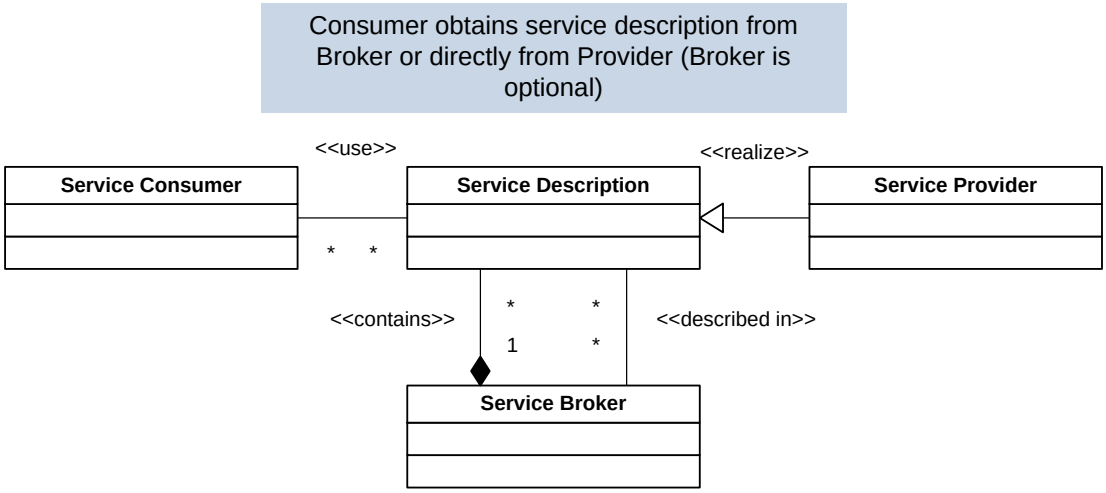


Figure 6 – Conceptual model of a SOA Architecture Style (Arsanjani, 2004)

It is important to understand and research security mechanisms in context to the broker architecture. Security is also influenced by the stakeholders to a great extent, as they tend to exchange information through other communication channels which are informal in nature e.g. phone, email, chat etc, which cannot be monitored through information systems and henceforth, will not be considered for the integrated security model.

Another important aspect is the level of service abstraction to be considered for this thesis. As this thesis intends to resolve the issues of security at a conceptual level, we shall not consider the technical aspects like web-services etc. As shown in the SOA layered architecture framework (see figure 7), we shall consider services (layer 3) as the basic layer of abstraction. The service layer and the layers above i.e. business composition, integration, governance etc. provide interesting perspectives which are considered in this thesis for solving the problem of security.

The next step is to delineate the relationship between SOA and extended CIA and to see to what extent can the principles of extended CIA be satisfied by SOA. CIA proposes a closed world i.e. by restricting the number of people who have access to the service and where confidentiality, integrity and accessibility are respected. On the other hand, interoperability and co-operability proposes an open world i.e. open service environment. It is important to maintain the balance between these two aspects and regulate each of these as required.

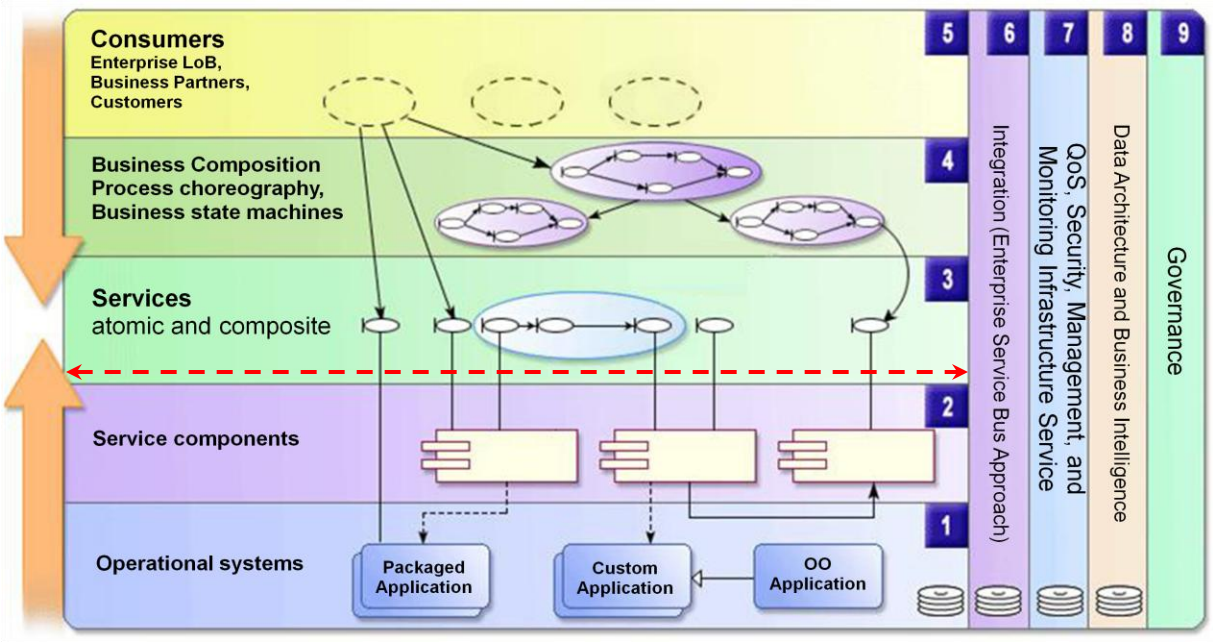


Figure 7 – SOA Layered Architecture Framework (IBM, 2008)

2.3 Model construction

The integral aspect of this study is to define a generic integrated security model for SOA with an insight of designing SOA architecture systems. The first step would involve identifying the strengths and inherent weakness of the CIA triad in order to formulate an integrated security model i.e. the extended CIA model.

Secondly, other theoretical views on the subject have to be considered with efforts to create an integrated security model in the context of SOA architected business environment. At the same time, acquisition of empirical information for the aforementioned aspects will be prepared. In this way we can establish the grounds for comparing the theoretical and empirical views of integrated security.

2.4 Model verification

The purpose underling the normative aspects of the inquiry are to create queries for the proposed model that can be verified and validated by the means of the empirical process. The empirical process will be conducted through a survey by using a questionnaire.

The model is valid because it is relevant with the existing knowledge concerning the issues of security and SOA. The model is fruitful because it is relevant to the purpose of the study. The empirical model is reliable because it represents the intellectual views of the people that have been interviewed. There is a mutual dependency between the theoretical model and the queries of inquiry. A model is complete if it is delineated by the queries of the study and the queries are relevant if they are derived from the model (Bubenko, 1978).

The questionnaire will provide us valuable inputs in order to improvise the model, whilst it would also help us to verify (i.e. identifying similarities and differences) the security model. The questionnaire will also try to combine and qualitative[8] and quantitative[9] approaches by using a "mixed method research" or "mixed-mode methodology" which attempts to combine both these approaches. The mixed-mode methodology provides a better understanding of the research problem and enhances the integrity of the research, as it complements quantitative and qualitative approaches. This corroboration also ensures the completeness and validity of the research. According to Metzler & Davis (2002), the choice of a mixed-mode approach was made 1). to compensate for the complexity of the subject matter and 2). with a desire to create a survey tool that would be concise and acceptable to the transit industry. The mixed-mode methodology process can be illustrated by the figure below (see figure 8), which is used in this thesis. This process is also popularly referred to as triangulation[10] in literature.

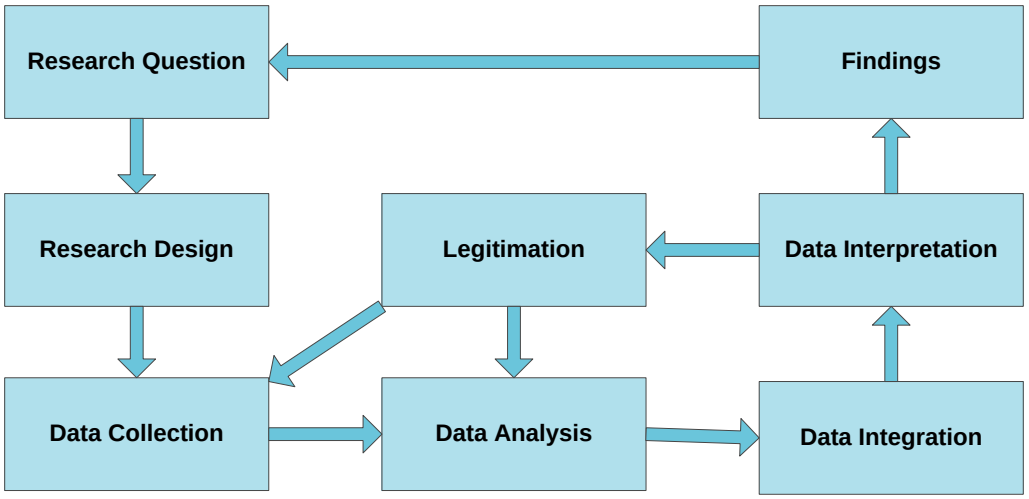


Figure 8 – Mixed research process model (Johnson & Onwuegbuzie, 2004)

[8] Qualitative research explores attitudes, behavior and experiences through such methods as interviews or focus groups. It attempts to get an in-depth opinion from participants (Dawson, 2002).

[9] Quantitative research generates statistics through the use of large-scale survey research, using methods such as questionnaires or structured interviews (Dawson, 2002).

[10] Triangulation is an approach to data analysis that synthesizes data from multiple sources. Triangulation combines information from quantitative and qualitative studies, incorporates prevention and care program data, and makes use of expert judgment. Triangulation methodology provides a powerful tool when a rapid response is needed, or when good data do not exist to answer a specific question (UCSF, 2008).

2.5 Derivation of partial and final conclusions through comparison

The empirical study is designed in such a way as to present the respondents with various answer options and then opinions are gauged with the help of a rating scale. The average rating will be considered to plot a radar chart as discussed in the section below.

The comparative part of the study outlines the similarities and differences between the theoretical and empirical views. Both these views are juxtaposed in a tabular format in order to derive partial conclusions of concerned issues. The partial conclusions have provided the sound grounds and corroboration for the final conclusions of this thesis work. Accordingly, we believe that we have conceived an answer to the security issues in a SOA environment that promotes an understanding of how SOA, expanded-CIA and SOA governance are related to each other. The final result of the study is an integrated security model that focuses on a secure, collaborative and attractive service environment.

2.6 Presentation of the comparison results

Radar charts are used for the graphical presentation of the results. These charts help us to differentiate between the theoretical possibilities and the empirical actualities as shown below (see figure 9). It also helps the reader to understand and interpret the conceptual information easily.

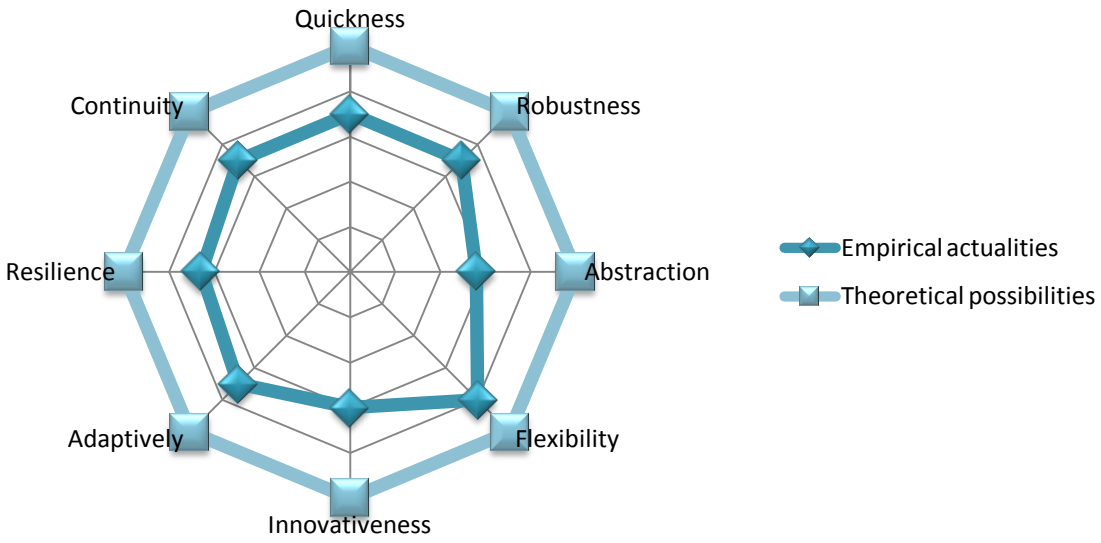


Figure 9 – Graphical presentation of the comparison results

3. Theoretical views of a SOA originated environment with respect to CIA

In this chapter we describe the properties of SOA and how these correspond with the security goals of CIA. This is followed by identifying additional security requirements of SOA which are assimilated by studying already existing SOA security models. Finally, we conclude this chapter by accruing an integrated model of SOA Governance with the security goals of SOA.

3.1 Properties supported by SOA (The Architectural Integrity of SOA)

SOA is a philosophy used in the design of concrete software architecture. The SOA environment is configured with respect to known or unknown customers, known providers and a broker. The broker aims to inform customers about the services that a particular provider can supply. In many cases, the composition of a process aiming to deliver something to a customer is composed by the activities of more than one provider. SOA allows for interoperability between heterogeneous systems and this is a case of customization that is very critical in the case of SOA.

The coordination of activities involved in the delivery of services follows either an orchestration strategy or so called choreography strategy. In the first case, one of the involved providers becomes responsible for coordinating the activities. However in the case of choreography, a constituent actor knows when it shall come into the environment do something and when it shall leave outside the environment.

The most elementary activity involved in the composition of the process is an elementary function. Such a function is represented as a black-box for the outside world as it is not necessary to know its internal logic. However, what is necessary to know is it's loosely dependencies to other functions from both the input side and the output side.

The properties and design principles of SOA have been elegantly discussed by Artus(2006), Jossutis(2007) and Erl(2008) in their respective books. Some of the important properties supported by SOA are listed below;

1. **Requisite of Agility and Loose coupling:** Loose coupling is the foundational characteristic of SOA because it declares neither chaos and information islands nor bureaucratic order and rigid interdependencies. One of the key aspects of SOA out of a holistic approach is agility. Agility requires loose coupling between;

    a. Various service providers
    b. Service providers and service consumers
    c. Service broker and service providers / service consumers.

The service consumer must be insulated from the details of the business logic implemented by the service provider and vice-versa. Any changes made to service provider, for e.g. redeployed in a different platform should not affect the service consumer in any manner. The same holds for the service broker which should function independently of the service provider and consumer.

Agility is a multi-dimensional concept (Alberts & Hayes, 2005) and it manifests itself into many other properties with respect to SOA;

- **Quickness:** To be quickly responsive in meeting the demands of the environment.

- **Robustness:** This means that independently of any turbulent conditions the processes should continue to function and be more efficient and useful.

- **Abstraction:** This emphasizes the need to hide as much of the underlying details of a service (Erl, 2008). This helps to enable and preserve the previously described loosely coupled relationship.

- **Flexibility:** To be flexible by providing the environment alternative ways to satisfy the demands of a customer. Flexibility can be understood in terms of a point-to-point pattern between providers and consumers or a broker centric option (Alberts & Hayes, 2005). Flexibility can be accomplished by making allowable design changes i.e. either in terms of introducing modules or modifications or by withdrawing existing modules. In the same sense flexibility can be given in terms of fluid relationships between modules (Henderson & Clark, 1990). The presupposition here is that the resulting pattern should always be both "simple" and comprehensible. This means that the number of connections between the entities (modules, systems, groups etc.) should be less than the number of its constituent objects.

- **Innovativeness:** To be innovative by providing new ways to perform a particular task, whilst improve existing ways to do more things.

- **Adaptively:** To be adaptive that is when large changes are made within the SOA environment it must adapt to the new conditions. For e.g. changes in business, politics, cultural, social, ecological etc. Achieving the appropriate level of agility requires that practical considerations be balanced against various design preferences.

- **Resilience:** To be resilient or perhaps reconciled that means in case of a catastrophic situation the strategy should shield the system and should facilitate recovery of the system back to its normal conditions as soon as possible.

- **Continuity:** To satisfy the conditions of business continuity which means in the case the providers of the services uses computers and computer networks, the enterprise of the

business continue to make business with or without the efforts of such technological infrastructure.

2. **Requisite of Visibility or Discoverability:** In order to call a service we need to know as to where the service exists. The service is usually advertized in the public domain where the service consumers can search and discover the service. A service can also be discovered through word of mouth. Service visibility becomes extremely critical when we have a complex service infrastructure with a complex mix of tools, processes and technologies.

3. **Requisite of Granularity or Composability:** The ability to effectively compose services is a critical requirement for achieving the fundamental goal of SOA. Services are expected to be capable of participating as effective composition members, regardless of whether they need to be immediately enlisted in a composition (Erl, 2008). Granularity can be defined as the degree of modularity of a system i.e. number of coarse grained operations a service should have. This also directly affects the number of service calls required to perform an operation. Artus (2006) states that, "in order to select the service granularities we are likely to be trading off factors such as maintainability, operability and consumability".

Some of the design principles of SOA specified in literature are controversial and sometimes conflicting in nature. There are listed below;

4. **Requisite of Consistency:** There are many candidate technologies available today for creating, publishing, discovering, and invoking services. SOA should provide a reference architecture specifying particular mechanisms that service providers and consumers will use such that there is consistency across all participants in the SOA (Artus, 2006). Henceforth, consistency helps reduce development, integration, and maintenance effort.

5. **Requisite of Statelessness:** Services are ideally designed to remain stateful only when needed. This is one of the most confusing aspects of services because some state is always involved. Services may be stateless from a business point of view and stateful from a technical perspective and vice-versa (Jossutis, 2007). A stateless service is a service that does not maintain any state between different service calls i.e. after the service call is over, the pertaining information which have been created temporarily to run the service are thrown away. Whereas a stateful service is a service that maintains state over multiple service calls. This aspect can also be referred as Transactional integrity i.e. either a service oriented transaction is correct/valid and hence it is wholly accepted or it is invalid and hence wholly rejected.

6. **Requisite of Reusability:** The common business case for SOA is that it leads to better reusability because all service consumers that need a particular functionality just have to call the same service provider. This is extremely beneficial but has certain limitations due to the trade-offs with performance. For instance, the issue with granularity i.e. if the services are fine grained it implies that the service calls are also fine grained which leads to an increase in the processing time. On the other hand if we have large amounts of data to process, the performance concerns may require us to use finer-grained services.

However, it is not sure if all the above principles define the architectural integrity of SOA environment. Accordingly, if some of the above principles are removed without any implication on the fundamental principle of SOA (for instance reusability), then this principle does not belong to the architectural integrity of SOA. Finally, this study focuses on the integration of SOA with CIA and not with the architectural integrity of SOA.

3.2 The idea of a secure service environment and outline of security requisites according to CIA

SOA is being increasingly used to architect systems in the IT industry, as they provide a way of building loosely-coupled services and also linking them within and across enterprises. A key benefit of this emerging architecture is the ability to deliver agile, integrated and interoperable solutions. At the same time ensuring the security of the environment is critical, both for organizations, their customers and other stakeholders.

The global and pervasive security requirements of any given information system are Confidentiality, Integrity and Availability (CIA). A key aspect of Information Security is to preserve the confidentiality, integrity and availability of an organization's information processing and networking. It is only with this information that it can engage in commercial activities. Loss of one or more of these attributes, can threaten the continued existence of even the largest business enterprises.

3.2.1 Confidentiality

Confidentiality is the characteristic or assurance that information is being shared only among authorized persons, entities and processes at authorized times and in an authorized manner. Confidentiality is said to be breached when any of the above criteria are not met and hence results in information being disclosed. The disclosure can take place by various means like printing, copying, e-mails or creating documents or even through word-of-mouth.

Confidentiality can be enforced by defining appropriate access levels for information. This involves segregating information into discrete items organized by "who should have access to it". It is also necessary to organize information based on its sensitivity i.e. the damage one would suffer if confidentiality was breached. Confidentiality is the key design goal of any cryptosystem[11], which is implemented using cryptographic techniques.

Confidentiality is also an ethical principle which is inculcated by professionals in various areas like medicine, law, journalism etc. There are numerous laws in place which state that the communication between the two parties (a person and one of the professionals) is confidential and may not be disclosed to third parties.

[11] The term cryptosystem is used as shorthand for "cryptographic system". A cryptographic system is any computer system that involves cryptography (Source: Wikipedia).

An example which illustrates the importance of confidentiality is health care, where it is considered as a fundamental tenet. It is increasingly difficult to maintain confidentiality in this era of computerized record keeping and electronic data processing which includes email, faxing patient's information, third party payment for medical services and sharing of patient care information among numerous health professionals and institutions (Synder & Leffler, 2005). An important aspect of medical care is to respect the privacy of patients, encouraging them to seek medical care and discuss their problems candidly. Confidentiality also ensures that patients are not discriminated on the basis of their medical conditions. A research conducted by the Duke University (2001) shows that for patients with HIV, breaches in confidentiality may result in discrimination, lesser quality health care or the loss of their home, job, health insurance and family.

3.2.2 Integrity

Integrity is the characteristic or assurance that a given piece of information is timely, accurate, authentic and complete. Integrity acts as a primary indicator of security in information systems (GASSP, 1999). Integrity is usually enforced using a set of rules or constraints which is inherent in any information system. As integrity refers to the validity of data, user account controls should not be inappropriately modified because even a momentary change can lead to service interruptions and result in breach of confidentiality. Other data such as user files must be available for modification, but should be reversible, for e.g. in the case of accidentally deleting important data. Integrity can be ensured by making use of digital signatures[12] which are equivalent to traditional handwritten signatures allowing the sender to verify his identity.

An example which illustrates the importance of integrity is in the area of research[13], where it is extremely vital. According to Synder & Leffler (2005), Integrity must govern all stages of research, from the initial design and grant application to publication of results. Investigators and the respective institutions are responsible both individually and jointly for ensuring that the obligations of honesty and integrity are met.

3.2.3 Availability

Availability is the characteristic or assurance of information and supporting systems being usable and accessible on a timely basis. It requires the systems responsible for delivering, storing and processing information to be accessible when needed by other systems or stakeholders which need them. Availability is also an assurance that relevant information should be provided to the client of the

[12] A digital signature or digital signature scheme is a type of asymmetric cryptography which gives the receiver the reason to believe the message was sent by the claimed sender (Source: Wikipedia).

[13] Research is defined under the federal "Common Rule" as "a systematic investigation including research development, testing and evaluation, designed to develop or contribute to generalizable knowledge" (Department of Health and Human Services, 2005).

service, devoid of the annoyance of information overload[14]. There are systems today with computing resources whose architectures are specifically designed towards improving availability. Depending on the specific system design, it might target power outages, network outages, upgrades, and hardware failures to improve availability.

An example which illustrates the importance of availability is in the case of airline booking systems. These systems need to be available online on a 24/7 basis, which is both an IT and business imperative. These systems must also be able to anticipate threats (for instance, high traffic during vacations) remain fault-tolerant[15] and maintain uptime.

3.3 Existing Models of SOA Security

In this section we shall review existing security models which cater to the requirements of the SOA environment. This will help us to derive the basis of for our model and also the key aspects of these models will be incorporated in our model.

3.3.1 NASA: Security Enhanced Model for SOA

According to Pajevski (2004), SOA security issues can be resolved by mitigating risks caused by the increased exposure of services by using a two-fold approach. Firstly, to use a proxy service to insulate services from consumers and to split the service registry into public and private areas. By using this technique we can debilitate and also to an extent eliminate direct attacks. Secondly, by using access control techniques which limits what the users can do, whilst also limits the harm they can cause.

From the figure below, we can see that that the classic SOA Model (as shown in figure 10) has been upgraded with a set of proxy services;

- A public service registry for consumers which provides the location of all services.
- A private registry service for proxy and other trusted entities which lists the actual location of each provider.

We can see that all requests go through the proxy service and the proxy gets authorization before forwarding any requests. Also, the messages will be checked for its format and any malicious content.

[14] Information overload refers to an excess amount of information being provided, making processing and absorbing tasks very difficult for the individual because sometimes we cannot see the validity behind the information (Source: Wikipedia).

[15] Fault-tolerance or graceful degradation is the property that enables a system (often computer-based) to continue operating properly in the event of the failure of (or one or more faults within) some of its components. Fault-tolerance is particularly sought-after in high-availability or life-critical systems (Source: Wikipedia).

Proxies can also augment the service with enhanced capabilities like load-balancing[16], quality of service[17] (QoS) etc. Also, note that the system could have only one service registry, which reports different service locations depending on whether the requestor is a trusted proxy or not.

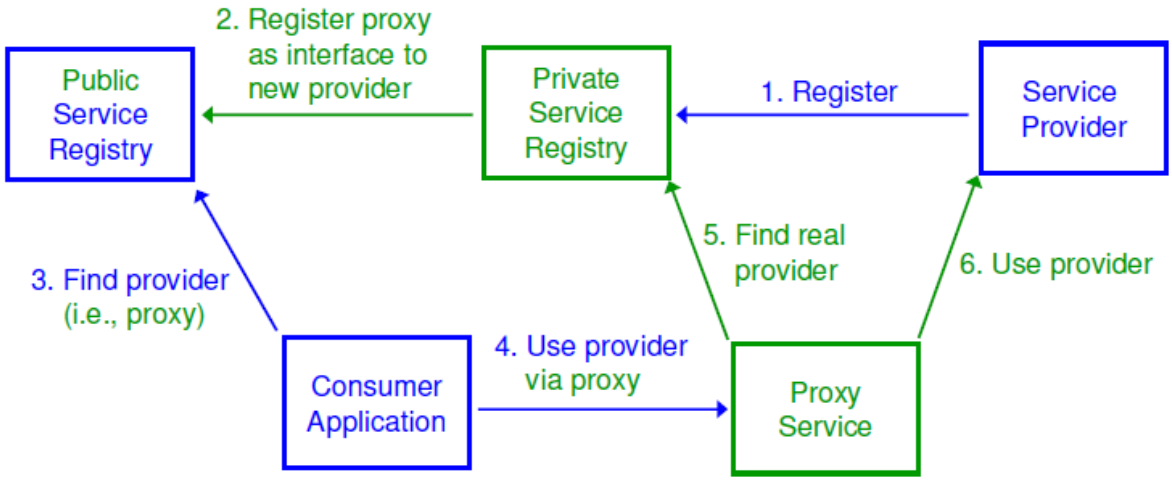


Figure 10 – A "Security Enhanced" SOA Interaction Model (Pajevski, 2004)

3.3.2 IBM: SOA Security Reference Model

Nagaratnam et al (2007), define a SOA security model (see Figure 11) as a list of enabling capabilities. Here, the capabilities refer to the IT and business security services, enablers and supporting infrastructure. They suggest that a reference model helps to address requirements and lead to a logical architecture and then to a physical architecture, with products and technologies mapped to solve the problem. The reference model can be classified under three layers of abstraction described below (Nagaratnam et al, 2007);

- **IT security services;** These are the foundational building blocks for a SOA infrastructure, providing the ability to secure the services and meet the needs of applications and infrastructure. These include services like identity service, authentication service, authorization service etc.

- **Security policy infrastructure;** This infrastructure entails articulating, managing, enforcing and monitoring security policies. This includes the ability to authenticate and authorize

[16] In computer networking, load balancing is a technique to spread work between two or more computers, network links, CPUs, hard drives, or other resources, in order to get optimal resource utilization, maximize throughput, and minimize response time (Source: Wikipedia).

[17] In computer networking, quality of service (QoS) is the ability to provide different priority to different applications, users, or data flows, or to guarantee a certain level of performance to a data flow (Source: Wikipedia).

requesters to access services, audit and protect information. Thus security policy management functionality is a core part of providing security capabilities in an SOA environment.

- **Business security services;** These services involve managing the needs and requirements of the business, such as identity and access management, data protection, governance and compliance. They help to effectively manage the relevant policies applicable to meet the business needs.

- **Security enablers;** These include technologies like cryptography, directories etc. that would be utilized by the security services to perform their task.

Governance and risk management provide the mechanism to implement and enforce security policies within the larger SOA environment (Nagaratnam et al, 2007).

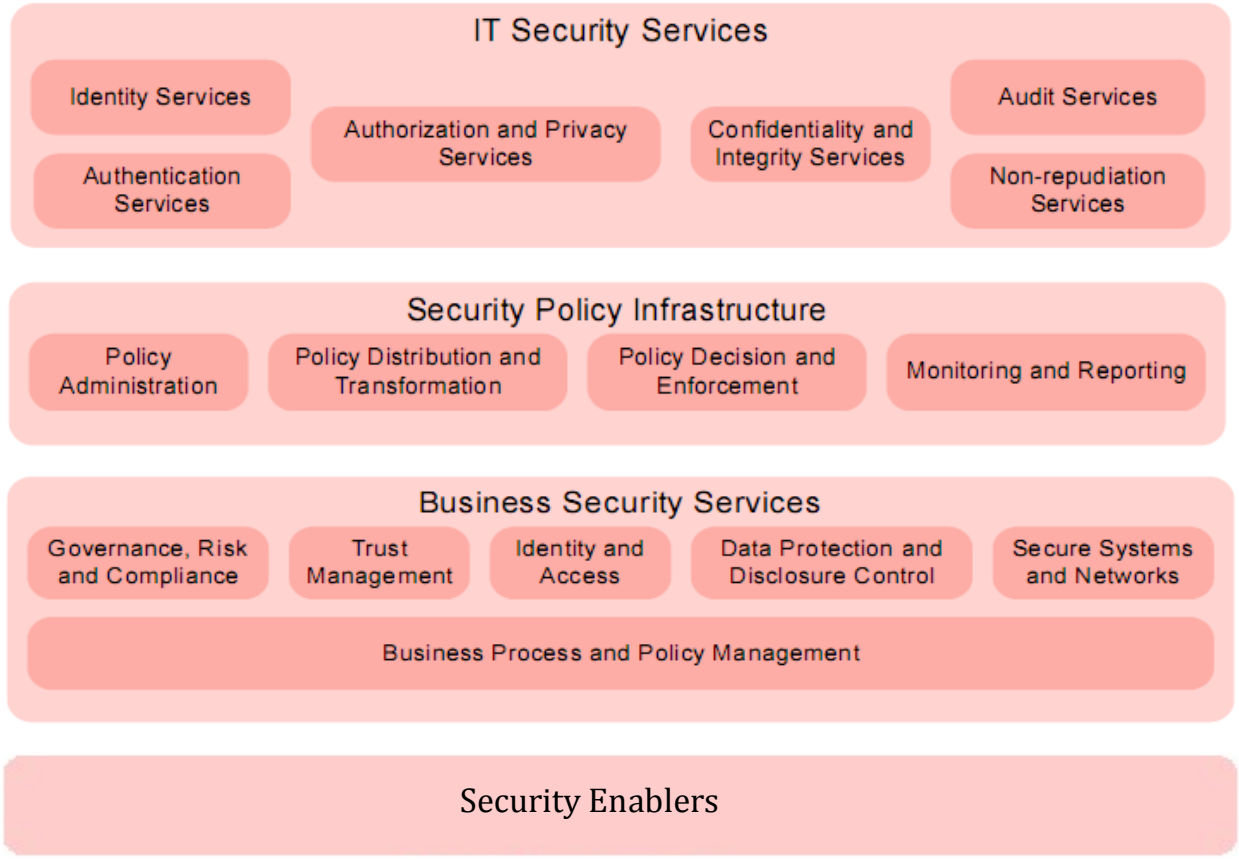


Figure 11 – SOA Security Reference Model (Nagaratnam et al, 2007)

3.3.3 CTC: SOA Security Model

CTC[18] defines a conceptual model for SOA as illustrated in the figure below (see figure 12). CTC describes security as an inherent aspect of SOA functionality. The key objective is to minimize external attacks and to secure all interactions between the constituent stakeholders. All the users of the information system must be identified and authorized in order to access any of the resources. The information assurance process is automated by using services like auditing which directs all required audits to a federated[19] audit service, an alert service which automatically sends real-time alerts to pertinent users (Youmans, 2008). The processes like identification, authorization, alerting and federation are implemented by various supporting technologies.

This security solution tracks and compares user attributes and data attributes to check for matching attributes before granting access to a resource. Finally, the SOA environment has to be evaluated for common security concerns like CIA and interconnected requirements.

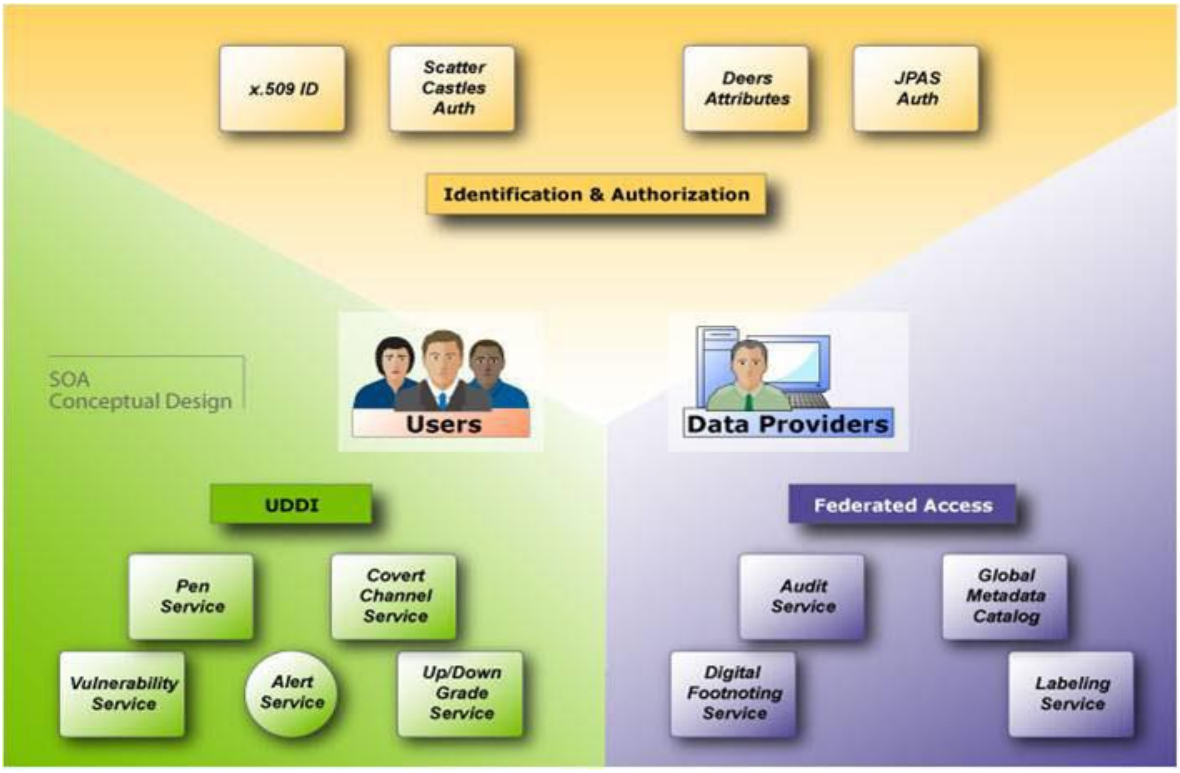


Figure 12 – SOA Security Reference Model (Youmans, 2008)

[18] Concurrent Technologies Corporation (CTC) is a non-profit organization which has been supporting a wide range of high-priority defense requirements and helping U.S. industry compete in the global market (Source: www.ctc.com).

[19] Federation is a method of replicating the same service to different sets of hardware, presumably in different physical locations (Youmans, 2008).

3.3.4 NSTISS: Comprehensive model for securing Information Systems

The NSTISS[20] committee defines "a comprehensive model for the security of information systems which also functions as an assessment, system development and evaluation tool" (NSTISS, 1994). This three-dimensional model illustrated below (see figure 13) attempts to address all security issues in an information system. The three layers of security measures can be utilized to minimize vulnerabilities based on the threats to an information asset. There are several applications of this model which are listed in the sections below.

A user can make use of the model to identify vulnerabilities pertaining to the critical information characteristics (Confidentiality, Integrity and Availability). If a specific technology is available to fulfill one of these characteristics, the next logical step for the user is to determine the policy and practice, education, training and awareness etc. If a suitable technology cannot be identified, then the policy or practice must be adopted as the next likely solution. If none of these two layers can counter the vulnerabilities then as a minimum the awareness of this deficiency becomes important.

The model can also be used as an evaluation tool, where the evaluator identifies the different information states with the information system. After identifying all the states the evaluator can perform a review as discussed above. It must be noted that a specific vulnerability may be left unsecured if the evaluator determines that no threat to that vulnerability exists.

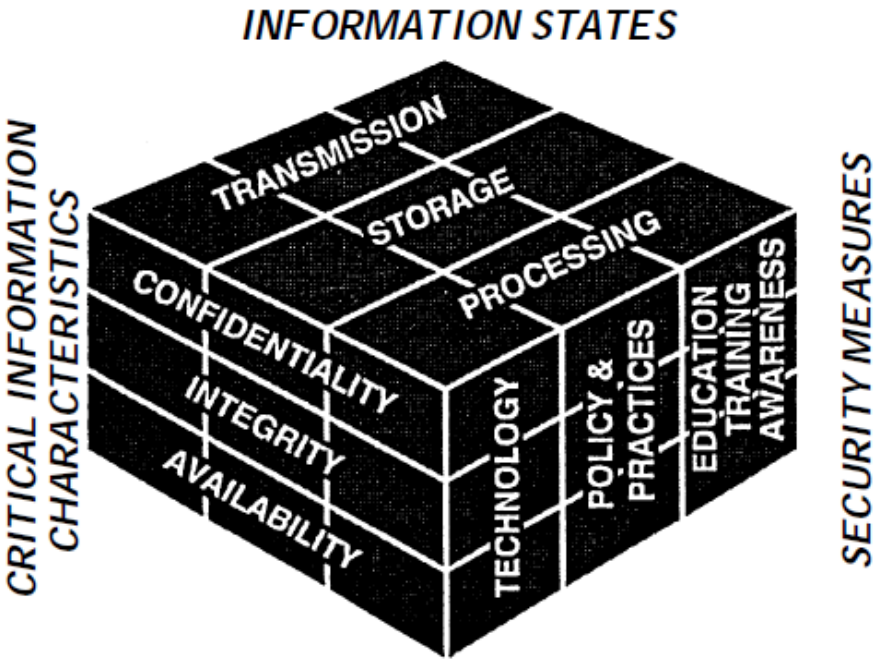


Figure 13 – Comprehensive Model for securing Information Systems (NSTISS, 2004)

[20] NSTISS is an acronym for National Security Telecommunications and Information Systems Security. This community mandates the development and implementation of a comprehensive approach to national security telecommunications and automated information systems security (NSTISS, 1992).

The twenty-seven individual cubes created by the model can be extracted and examined individually (NSTISS, 2004). This can be useful for categorizing and analyzing countermeasures for security. It also serves as a tool for defining organizational responsibility for information security. The NSTISS security model acknowledges information and not technology, as the basis for our securing information systems.

3.4 Other important requisites of security

From the various theoretical models described above we perceive that the complexity of SOA dictates additional security requisites that have to be satisfied in order to have a secure environment. These following aspects are standard security in the sense that they exist even with traditional applications as well. But, the context of these requirements drastically varies in the SOA environment.

3.4.1 Authorization

Authorization is a security concept where access to resources is allowed to only those who are permitted to use them. This is termed as access control and is usually determined by finding out if a person is a member of a particular privileged group i.e. if that person has the rights to access that resource, or has a particular level of security clearance.

Consider a composite application that combines the capabilities of multiple services. As an action the composite application may consist of multiple actions in constituent services, the composite application should ideally check the access control rules of all constituent services before initiating an action. But this is only possible if the access control rules of each constituent service are also available to the composite application.

3.4.2 Authentication

Authentication is the process of establishing or confirming the identity of a user. This usually involves a username-password combination, but can also include other methods of demonstrating identity such as a smart card or use of biometrics techniques like fingerprint reading, retina scan etc.

If the service is invoked within the same enterprise, we can use the corporate directory to authenticate users. But, if it is invoked from outside the enterprise, that repository is of no use. It is possible for authentication to be performed by a service and reuse it, but this might not work very well in all situations.

3.4.3 Identity

Identity is an essential attribute required to authenticate a user. Identity based security controls are necessary for SOA because they are not dependent on any single application design or technology (McAllister, 2004). Different mechanisms can be used to authenticate a user to a given identity. For e.g. passwords, digital certificates, encryption and biometric techniques etc. Also, the individual

services need not know anything about the underlying authentication system so long as they are satisfied with the validity of the user's identity.

In the case of a composite application, users might have to be individually authenticated and authorized for each of the constituent services if there is no mechanism to manage user-identities. The identity has to be managed for an entire session such that the user should have to login only once. This is usually accomplished by making use of Single Sign-on[21] (SSO) solutions or by making use of OpenID[22].

3.4.4 Auditing and Compliance

Security can be viewed as a three part process which involves protection, detection and response (Peterson, 2008). Most of the security requirements discussed till now are protection schemes. We need a requirement which helps us to detect security vulnerabilities and respond with suitable measures which involves Auditing. A system should be configured to track messages between services and generate usage logs during specific periods of time. This audit serves as an important record of what has happened that can be used to investigate problems and diagnose potential security weaknesses (Pulier & Taylor, 2005).

Compliance is the state of being in accordance with established guidelines, specifications and legislation. It's not just archiving, but the ability to access information that is essential for achieving compliance (Manoj, 2005). Every organization or enterprise has different service levels for different users, which drives information access, retrieval and disposition requirements. In essence, companies need to protect the right data longer, retrieve it as needed, and also discard it when it's obsolete.

3.4.5 Security Policies

Security rules, policies, procedures and guidelines help to maintain and address all aspects of information security. It also encompasses all the SOA participants i.e. clients, services, processes and infrastructure. GASSP (2005) states that, "it is essential that organizations establish, maintain and promulgate a clearly articulated hierarchy of policies and supporting standards including lines of authority and responsibility that address the security of information assets". Security policies can also include contract management where a contract (set of rules) is used to govern the use of a service (Pulier & Taylor, 2005). For e.g. a contract may stipulate that a particular user has the right to invoke a service five times per day. Additionally, it might also say that on invocation the service level must meet certain parameters such as a one second response.

[21] Single sign-on (SSO) is a method of access control that enables a user to log in once and gain access to the resources of multiple software systems without being prompted to log in again (Source: Wikipedia).

[22] OpenID is an open, decentralized standard for user authentication and access control, allowing users to log onto many services with the same digital identity. As such, it replaces the common login process that uses a login-name and a password, by allowing a user to log in once and gain access to the resources of multiple software systems (Source: Wikipedia).

The lack of policies and administrative controls could result in the organization divulging the information assets to risks and to increase the potential of loss or harm to the organization. Furthermore, the lack of policy could result in the lack of management options for remediating such a situation.

3.5 Towards a secure SOA Environment

From this chapter, we can surmise that security is a critical aspect of business and is no longer just about technology. The critical security requirements to secure an information system are Confidentiality, Integrity and Availability (CIA), but in the case of SOA we have additional requirements like Authentication, Authorization, Identity, Auditing and Compliance and Policy management. The real problem that has to be confronted is "What kind of security is required for SOA and Why?" For instance in the NASA's model, they focus on a secure provider because everything between services is based on message exchange and therefore they give a sound model by taking into account the security of providers. In principle, SOA main concern is the loosely integration of services. However dealing with a service is one thing and data is another. Therefore, we need to make more explicit the relationship between services in general and data in specific.

SOA environments may be classified to high-sensitive and low-sensitive with respect to the uses of security. High-sensitive environments are those that security must function otherwise it is not an idea to invest in information technology. For example healthcare environments, banking environments, military environments etc. Other environments such as library environments, recreation or entertainment service environments etc are characterized by low or moderate sensitivity.

An integrated framework for SOA Governance was proposed by K. Kingkarn in her thesis entitled "An Integrated model for SOA Governance" (Kingkarn, 2008). This integrated model facilitates the governance and management of the SOA environment. Here the concept of governance infers, exercising control over the service environment (standards, policies, contracts, quality etc.). Management infers to the process of creating (shaping, reshaping, evaluating, maintaining etc.) a service-based environment that holds together the domain of service providers, service consumers and service brokers. This model also promotes attributes such as change management and compliance which are extremely essential in the case of a heterogeneous and complex service-based business environment. Despite this elegant presentation of SOA Governance by K. Kingkarn, the issues of security have been not addressed. Neither the concept of SOA has been extended to include the aspects of security, nor does the concept of SOA Governance take into account any crucial issues of security.

This model can be updated to accommodate the various aspects of security (highlighted with red font in figure 14). In this sense, the model consists of four domains with the corresponding relationships between these domains. The domains we refer are;

- Secure informational tasks supported by proxy services.
- Domain of security politics.

- Domain of security measures, concepts and policies.
- Domain of security capabilities.

The internal relationships concern the conformity between the secure service environment and the other domains i.e. "conformity <=> alignment" between the corresponding domains. The external relationships consist of stakeholder expectations, stakeholder invested efforts and stakeholder education.

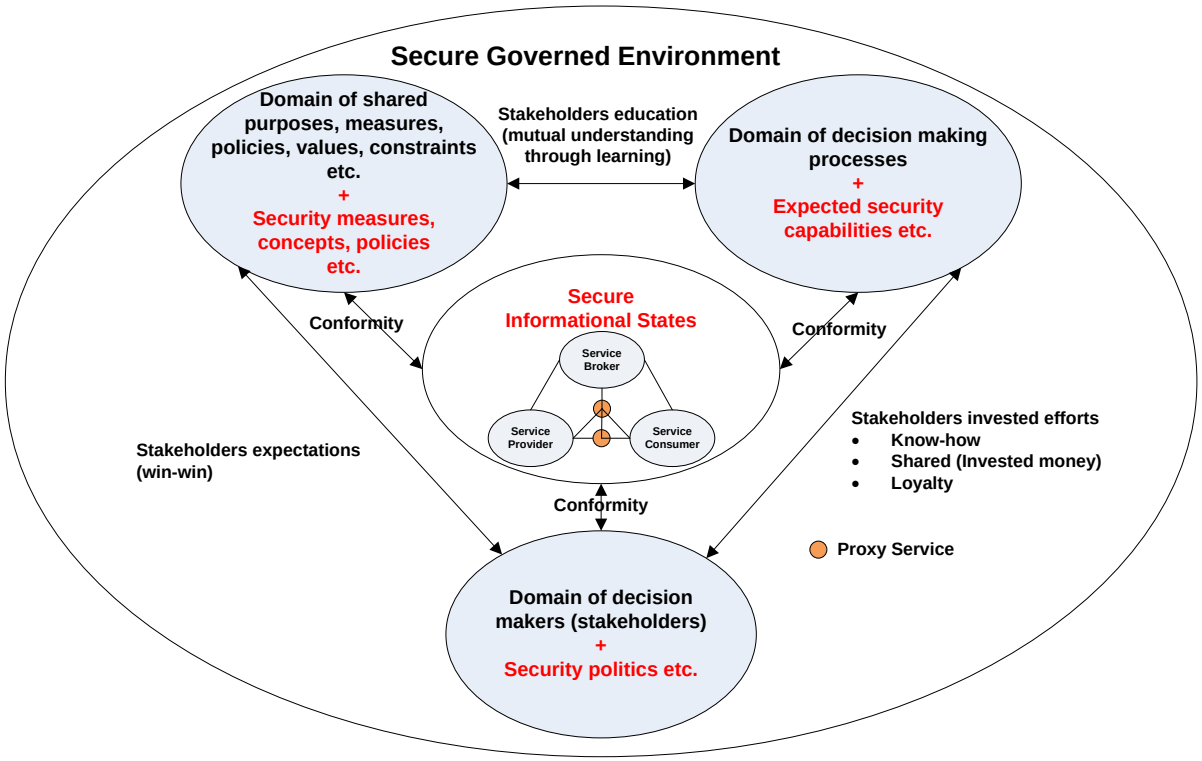


Figure 14 – The Extended Model of Secure-Governed Environment enabled with Proxy services (Own model derived from K. Kingkarn's original model)

3.6 A last word about the above model

A foundational difference of the security models described in this section is the so called proxy service. It means that there is no direct contact between the domain of service consumers, domain of service providers and domain of service brokers.

4. Creating an alternative model for SOA security

This section describes the foundation of an integrated SOA security model along with its composition. Then we describe the basis for the empirical inquiry, the design of queries to validate the model and finally the data collection method.

4.1 Foundation of the model

An integrated model for SOA security consisting of three dimensions i.e. security measures and concepts, informational tasks and capabilities are described below (see Figure 15). This model attempts to address all security issues in a SOA business environment as follows;

- The first dimension of the SOA security model consists of explicit security measures and concepts such as: Confidentiality, Integrity, Availability, Authentication, Authorization, Identity, Auditing and Compliance and Security Policies, etc.

- The second dimension of the SOA security model consists of informational tasks such as: Transport security, Message security, Application security, Data security, Knowledge security, Control security etc.

- The last dimension of the SOA Security model deals with the requisites of capabilities such as: Education, Training, Awareness, Mutual understanding, Practices etc.

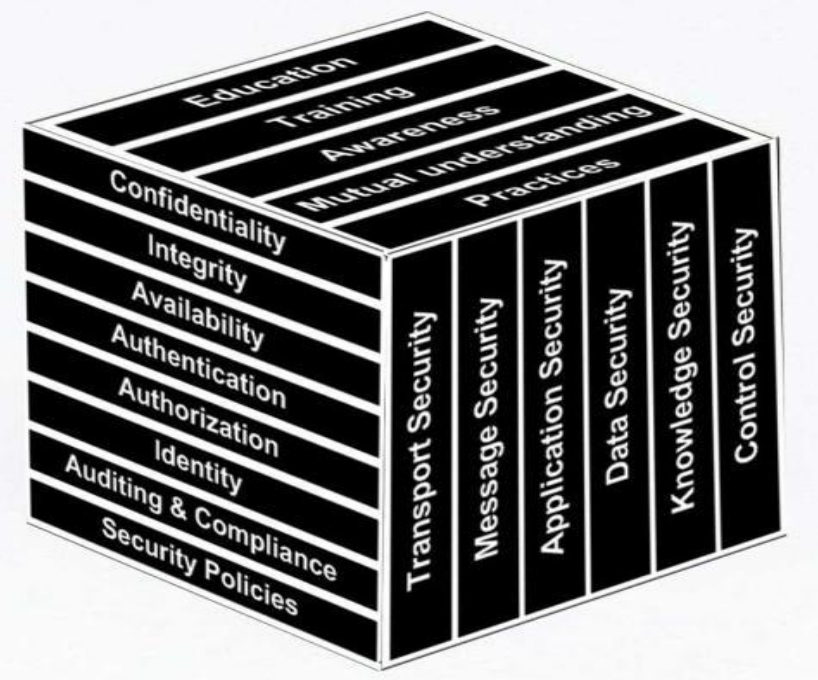


Figure 15 – The Integrated Model for SOA Security (Own model derived from the consideration of several ideas for integrating SOA and CIA)

4.2 Composition of the model

The first dimension of the integrated SOA security model consists of explicit security measures and concepts for securing a SOA business environment. These measures have to be deployed in such a manner that all the informational tasks are secured. The informational tasks form the second dimension of the model. This dimension encompasses information processing, information flow and information store. Finally, in the third dimension we represent the support level provided by the solution to the corresponding security measure and the Information task.

Each of the components of the first dimension (tuple of security measures and concepts) is directly related to the second and third dimensions (i.e. tuple of informational tasks and tuple of security capabilities);

- The tuple of security measures and concepts can be correlated with the tuple of informational tasks i.e. Confidentiality, Integrity, Availability, Authentication etc. can be enforced by implementing each of the components of Informational tasks like Transport security, Message security, Application security etc.

- The tuple of security capabilities can be used to empower the tuple of informational tasks i.e. Transport security, Message security, Application security etc. can be implemented by making use of Education, Training, Awareness etc.

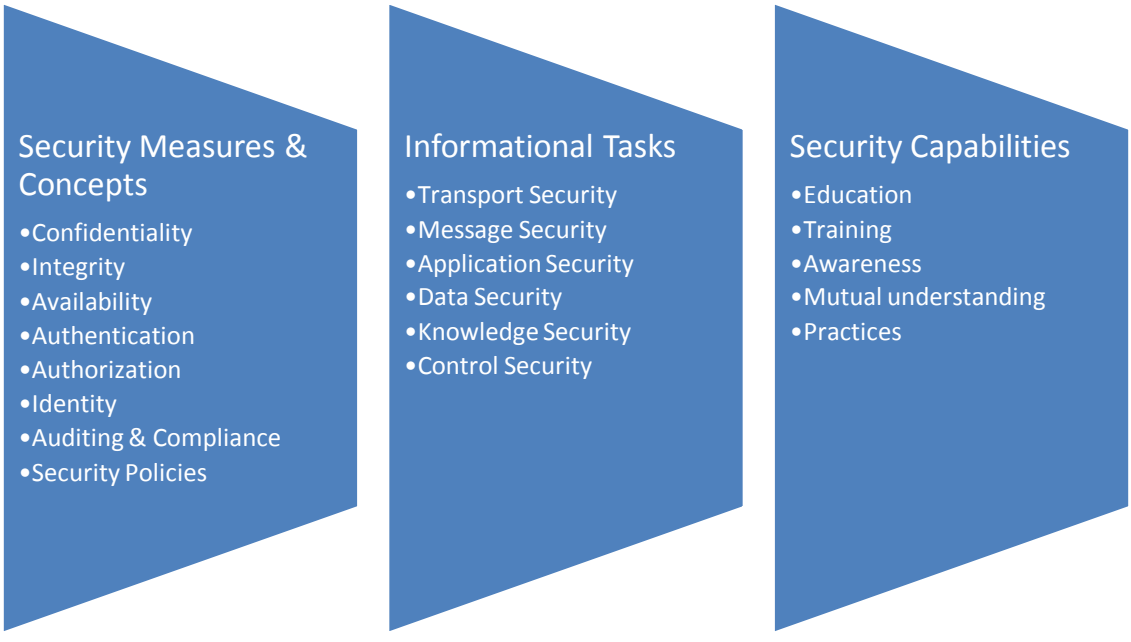


Figure 16 – Composition of the Integrated Model for SOA Security

4.3 Describing the empirical inquiry

As described in chapter 2, empirical inquiries will help to verify and validate the security model and help in proving its credibility. The inquiries will also help to improve and extend this model and hence serve as a learning tool. The empirical enquiries can be deduced based on the relationship between the domain of Informational tasks, domain of Security measures and concepts, and domain of Security capabilities (see Figure 16) as shown below;

- The queries Q1 - Q4 are based on the contextual understanding of the SOA environment.
- The queries Q5 - Q10 are based on the relationship between the domain of Informational tasks and the domain of Security concepts and measures.
- The queries Q11 - Q16 are based on the relationship between the domain of Informational tasks and the domain of Security capabilities.
- The queries Q17 - Q18 are based on the relationship between the domain of Security concepts and measures and the domain of Security capabilities.

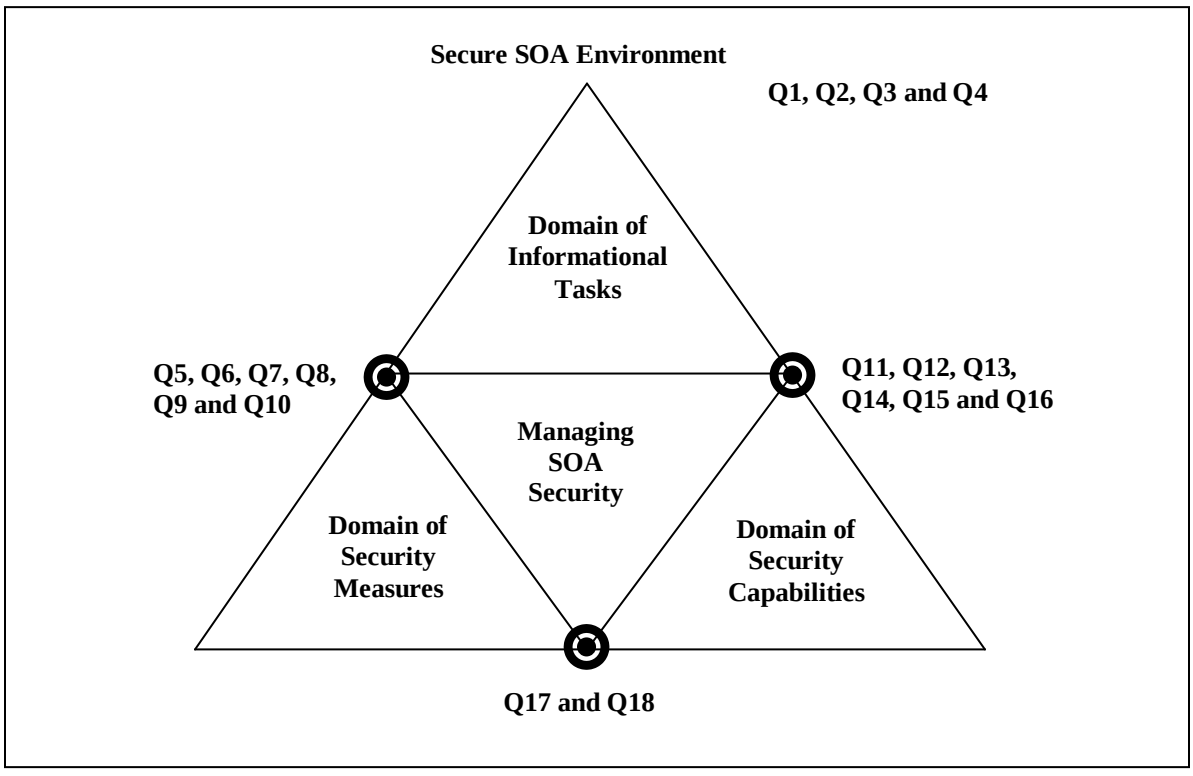


Figure 17 – Describing the empirical inquiry (own design)

The questionnaire consists of twenty questions which are listed in the next section. Some of the queries in the questionnaire consist of a rating scale which will are graded through five levels as described below;

0 – Not Important
1 – Marginally Important
2 – Moderately Important
3 – Extremely Important
4 – Blockbuster

In order to view the complete questionnaire, kindly refer to Appendix A - Questionnaire: Inquiring the Issues of SOA Security.

4.4 Data collection for the empirical inquiry

The data collection for the empirical inquiry was conducted by using a questionnaire. The respondents for this questionnaire were required to have some pre-requisite knowledge about the functionality of SOA and some basic understanding of security.

Totally six IT professionals were interviewed, below are the names, positions and their respective organizations;

S.no	Name	Occupation	Organization
1	Dr. Jonas Landgren	Research Manager	Viktoria Institute Gothenburg, Sweden.
2	Dr. Yun Lin	System Design Architect	Agresso AS, Oslo, Norway.
3	Mr. Krishna Raju	System Architect	Symbol Technologies, Bangalore, India.
4	Mr. Vikram Gururaj	Chief Technological Officer (CTO)	Seventy MM Bangalore, India
5	Mr. Shashidhar C. N.	Internal Consultant	IBM, Bangalore, India.
6	Mr. Pradeep J. V.	Programmer	FOI, Stockholm, Sweden

5. Systematization of the empirical views

In this chapter we systematize the empirical views which were collected by the use of a questionnaire (see Appendix A). The empirical queries and views are juxtaposed in the section below, followed by an analysis on the results.

5.1 Notations and agreement criterion

The empirical views were collected by interviewing six technical professionals (denoted by P1 to P6) who have some expertise working on SOA and also to an extent understand the requisites of security. An average rating is ascertained by taking into account all the individual ratings. The conformance of the results to the theoretical views is measured by using an agreement criterion as listed below;

Average rating 1 - 2, implies lack of agreement,
Average rating 2 - 3, implies low agreement,
Average rating 3 - 4, implies moderate agreement and
Average rating 4 – 5, implies strong agreement.

5.2 Detailed Analysis

Q1. Do you think it's a good strategy to insulate the direct contact between the service consumer and service provider?

Some models of SOA security make use a proxy service to insulate services from consumers and to split the service registry into public and private areas. The proxy services to an extent helps eliminate direct attacks and also augment the service with enhanced capabilities like load-balancing, quality of service (QoS), etc.

Criteria	**Empirical Answer (Yes/No)**						
	P1	**P2**	**P3**	**P4**	**P5**	**P6**	**Agreement**
Yes/ No	Yes	Yes	Yes	Yes	Yes	Yes	Strong

The answer to this query by all the interviewed professionals was unanimously 'Yes'. They further justified this with the following viewpoints;

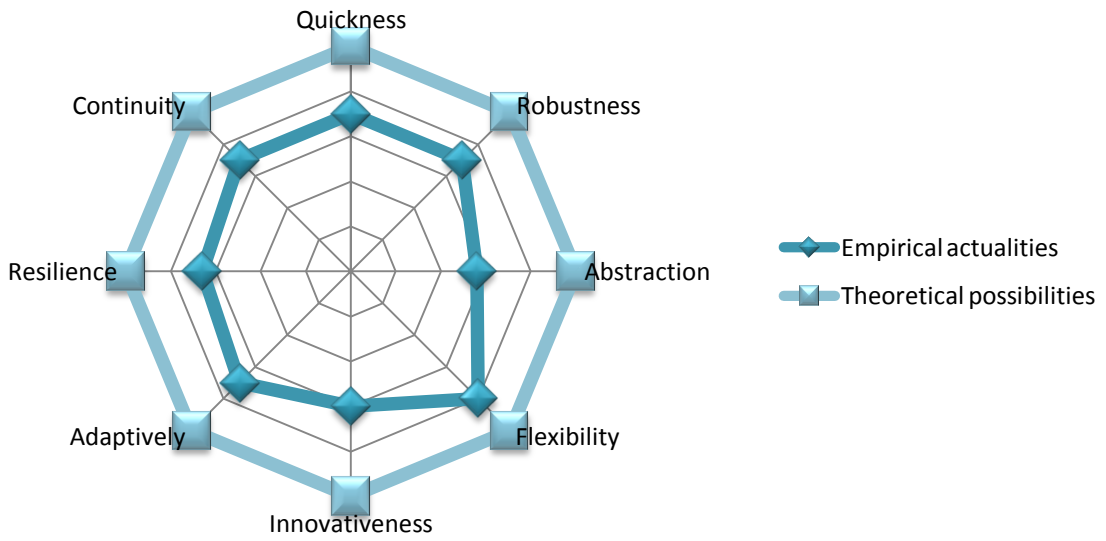
- A separation of core services is always favorable in order to provide flexibility and at the same time maintaining system stability.
- It enables service loose coupling and reusability in a secure way whilst direct attacks are eliminated.
- It helps in creating a layered approach to SOA security.

Q2. To what extent do the following properties significantly express the property of Agility?

Agility is one of the key property or design principle of SOA which also manifests itself into many other properties of SOA. It is important to identify to what extent these properties are aligned with respect to the property of Agility.

Criteria	Empirical Answer (Rating x/5)							
	P1	P2	P3	P4	P5	P6	Avg.	Agreement
Quickness	4	2	4	3	3	5	3.5	Moderate
Robustness	3	1	4	5	3	5	3.5	Moderate
Abstraction	3	2	3	3	3	3	2.8	Low
Flexibility	5	3	3	4	4	5	4	Strong
Innovativeness	5	1	2	3	3	4	3	Moderate
Adaptively	3	4	4	4	2	4	3.5	Moderate
Resilience	4	4	2	3	3	4	3.3	Moderate
Continuity	4	2	4	3	4	4	3.5	Moderate
Other	-	-	-	-	-	-	-	-

Info-graphics

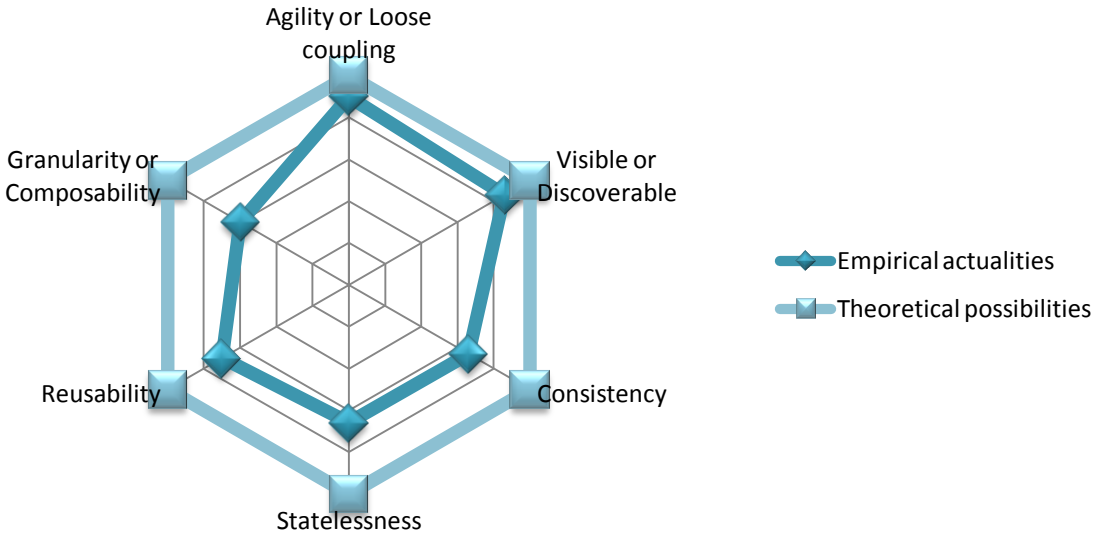


Most of the interviewed professionals have a varied view of Agility which is a core design principle of SOA. 'Flexibility' is determined as a strong match to Agility and 'Abstraction' as a low favored match. The other definitions of Agility have received mixed responses but are mostly positive.

Q3. To what extent do the following properties qualify to define the architectural integrity of SOA?

This question deals with the foundational properties or the design principles of SOA The understanding of these properties is vital as they play a role in shaping the SOA environment. The SOA environment follows the system of principles that together defines the architectural integrity of SOA. But, this does not exclude the situation where the system of principles is viewed inconsistent and therefore insufficient for determining the desirability of architectural integrity.

Criteria	Empirical Answer (Rating x/5)							
	P1	P2	P3	P4	P5	P6	Avg.	Agreement
Agility or Loose coupling	5	3	5	4	5	5	4.5	Strong
Visible or Discoverable	5	4	4	5	3	5	4.3	Strong
Consistency	3	2	4	4	3	4	3.3	Moderate
Statelessness	3	3	3	4	3	4	3.3	Moderate
Reusability	4	4	4	3	2	4	3.5	Moderate
Granularity or Composability	3	3	4	2	2	4	3	Moderate
Other	-	-	-	-	-	-	-	-
Info-graphics								

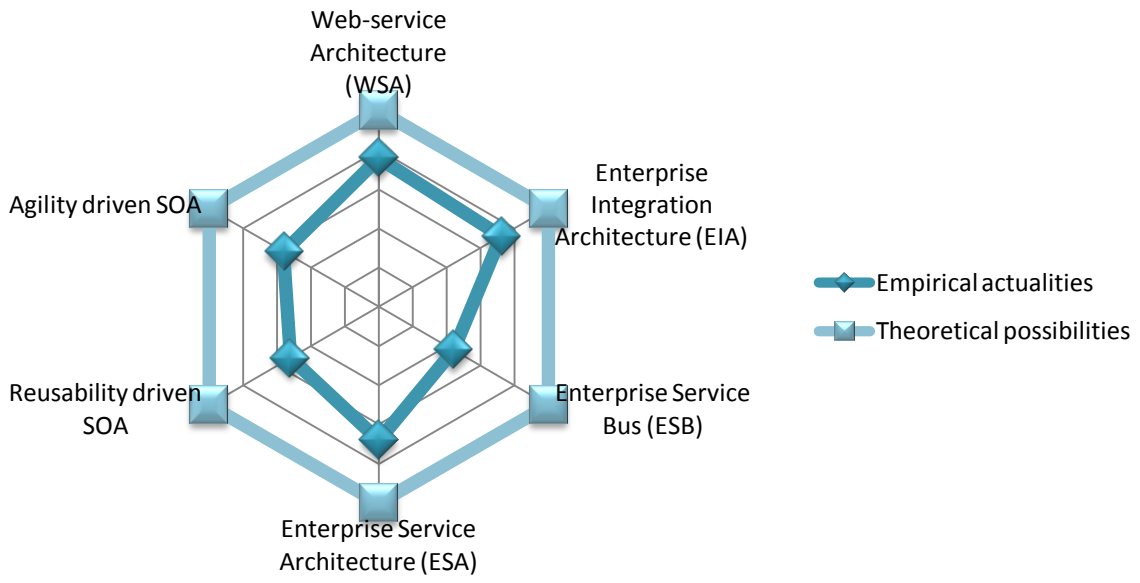


Empirically, Agility or Loose coupling and Visible or Discoverable are perceived to be the foundational properties of SOA architecture. The other properties like Consistency, Statelessness, Reusability, Granularity and Composability etc. must always be in harmony with the foundational ones.

Q4. To what extent are the following approaches relevant to the characteristics of an architecture that addresses the use of security?

The approaches listed below are the various design solutions of SOA. These approaches don't take into account security as a critical requirement and they are not always in agreement with the foundational principles of SOA.

Criteria	Empirical Answer (Rating x/5)							
	P1	P2	P3	P4	P5	P6	Avg.	Agreement
Web-service Architecture (WSA)	-	3	5	5	5	3	3.8	Moderate
Enterprise Integration Architecture (EIA)	-	4	4	4	3	3	3.6	Moderate
Enterprise Service Bus (ESB)	-	1	2	3	2	3	2.2	Low
Enterprise Service Architecture (ESA)	-	4	4	4	2	3	3.4	Moderate
Reusability driven SOA	-	2	3	3	2	3	2.6	Low
Agility driven SOA	-	2	4	3	2	3	2.8	Low
Other	-	-	-	-	-	-	-	-
Info-graphics								

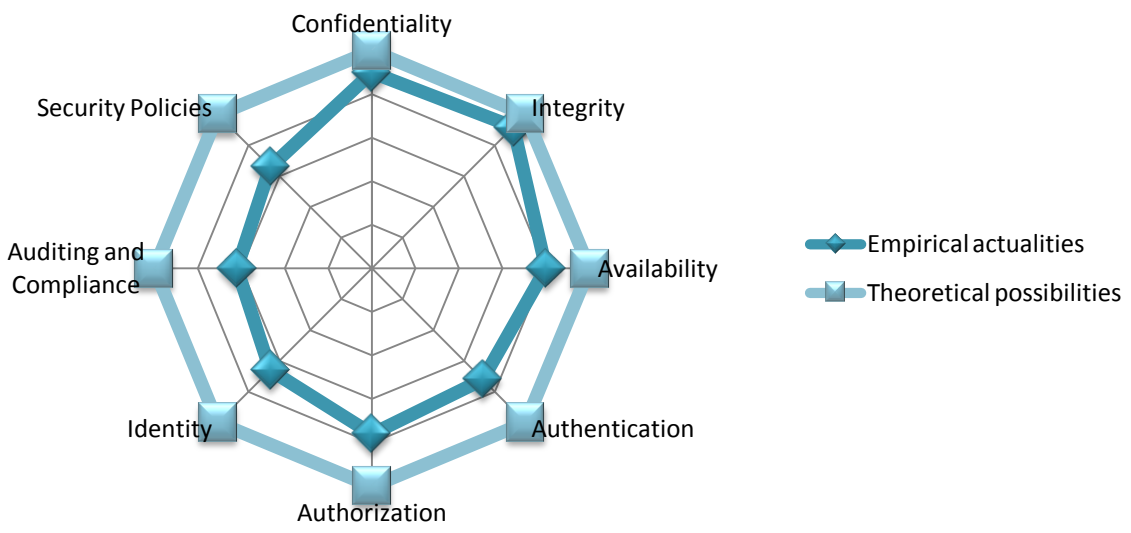


Though there are several design solutions of SOA, most professionals believe that WSA, EIA and ESA inherently address the use of security. The other design solutions like Agility driven SOA, ESB and Reusability driven SOA are considered more susceptible to be lacking security.

Q5. To what extent are the aspects listed below relevant and critical for Transport security?

Transport security is essential when the information is in transit i.e. when information is exchanged between the constituent services in SOA. This query determines to understand the significance of each of the security measures and concepts of SOA with respect to Transport security.

Criteria	Empirical Answer (Rating x/5)							
	P1	P2	P3	P4	P5	P6	Avg.	Agreement
Confidentiality	4	3	5	5	5	5	4.5	Strong
Integrity	4	4	5	5	5	5	4.6	Strong
Availability	5	3	3	3	5	5	4	Strong
Authentication	4	1	4	5	4	4	3.6	Moderate
Authorization	4	3	4	4	4	4	3.8	Moderate
Identity	3	2	3	4	4	4	3.3	Moderate
Auditing and Compliance	2	1	4	4	4	4	3.1	Moderate
Security Policies	4	0	4	4	4	4	3.3	Moderate
Other	-	-	-	-	-	-	-	-
Info-graphics								

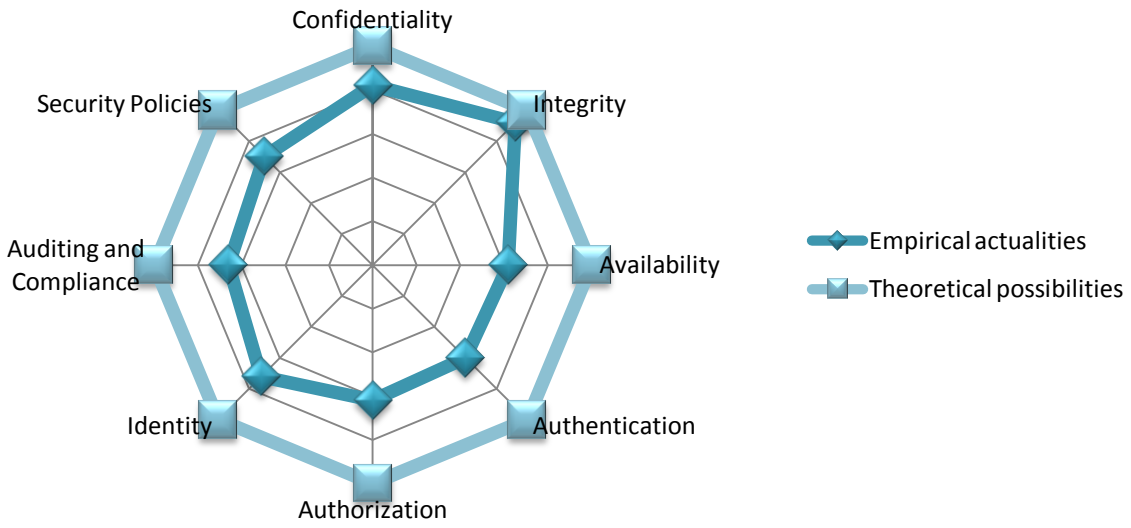


Confidentiality, Integrity and Availability were considered as the strong contenders for Transport security. This is followed by Authorization, Authentication, Identity, Security Policies and finally Auditing and Compliance.

Q6. To what extent are the aspects listed below relevant and critical for Message security?

The whole idea of SOA is based on messages exchanged between services. In the case of Message security all the information related to security is encapsulated in the message. The individual messages (request/response) are routed between service consumers, providers and intermediaries. This query determines to understand the significance of each of the security measures and concepts of SOA with respect to Message security.

Criteria	Empirical Answer (Rating x/5)							
	P1	P2	P3	P4	P5	P6	Avg.	Agreement
Confidentiality	5	3	3	4	5	5	4.1	Strong
Integrity	5	4	5	4	5	5	4.6	Strong
Availability	2	2	3	2	5	5	3.1	Moderate
Authentication	2	1	4	4	4	3	3	Moderate
Authorization	3	3	3	3	4	3	3.1	Moderate
Identity	5	3	3	4	4	3	3.6	Moderate
Auditing and Compliance	3	2	4	3	4	4	3.3	Moderate
Security Policies	4	1	4	4	4	4	3.5	Moderate
Other	-	-	-	-	-	-	-	-
Info-graphics								

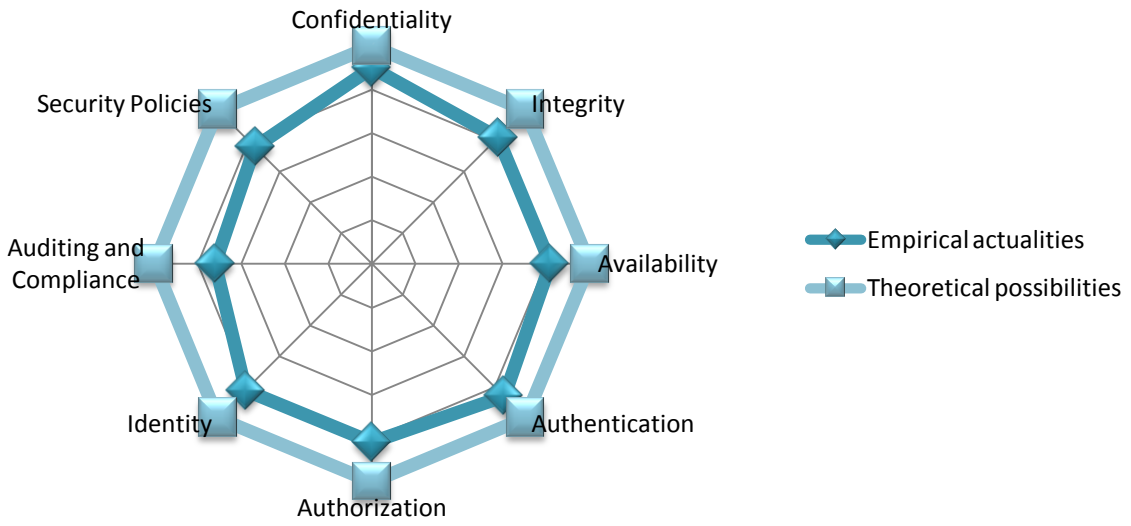


Confidentiality and Integrity were considered as the strong contenders for Message security. This is followed by Identity, Availability, Authorization, Security Policies, Auditing, Compliance and finally Authentication.

Q7. To what extent are the aspects listed below relevant and critical for Application security?

Application security involves using security measures and concepts to protect applications from external threats. This could involve security mechanisms that are directly coupled with the application logic. Security measures and concepts minimize the likelihood that hackers will be able to manipulate applications and access, modify, or delete sensitive data. This query determines to understand the significance of each of the security measures and concepts of SOA with respect to Application security.

Criteria	Empirical Answer (Rating x/5)							
	P1	P2	P3	P4	P5	P6	Avg.	Agreement
Confidentiality	5	3	5	4	5	5	4.5	Strong
Integrity	5	2	4	4	5	5	4.1	Strong
Availability	5	2	5	3	5	5	4.1	Strong
Authentication	4	4	4	4	5	5	4.3	Strong
Authorization	4	4	3	4	5	5	4.1	Strong
Identity	4	4	3	4	5	5	4.1	Strong
Auditing and Compliance	3	3	4	3	4	5	3.6	Moderate
Security Policies	3	4	4	3	4	5	3.8	Moderate
Other	-	-	-	-	-	-	-	-
Info-graphics								

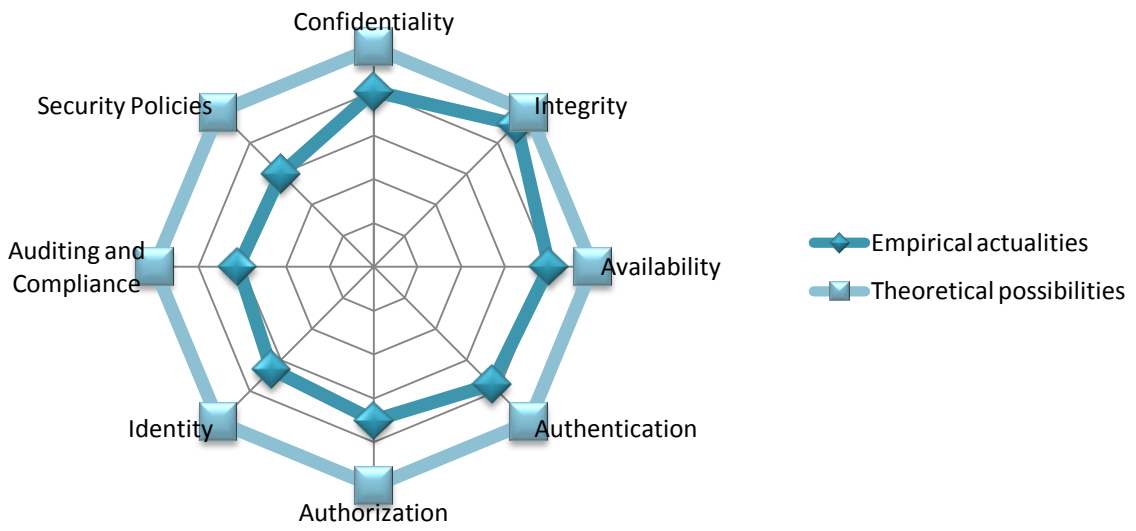


Confidentiality, Integrity, Availability, Authentication, Authorization and Identity were considered as the strong contenders for Application security. This is closely followed by Security policies, Auditing and Compliance. It is quite clear that most professionals perceive that Applications should be able to handle most of these security requisites.

Q8. To what extent are the aspects listed below relevant and critical for Data security?

Data security involves regulating access and ensuring that the data is safe from corruption or loss. It also helps in ensuring privacy and protecting personal information. This query determines to understand the significance of each of the security measures and concepts of SOA with respect to Data security.

Criteria	Empirical Answer (Rating x/5)							
	P1	P2	P3	P4	P5	P6	Avg.	Agreement
Confidentiality	5	1	5	4	4	5	4	Strong
Integrity	5	4	5	5	4	5	4.6	Strong
Availability	5	4	3	3	4	5	4	Strong
Authentication	4	2	4	4	4	5	3.8	Moderate
Authorization	4	2	3	3	4	5	3.5	Moderate
Identity	4	3	3	4	2	4	3.3	Moderate
Auditing and Compliance	3	4	4	3	2	3	3.1	Moderate
Security Policies	3	2	3	3	4	3	3	Moderate
Other	-	-	-	-	-	-	-	-
Info-graphics								

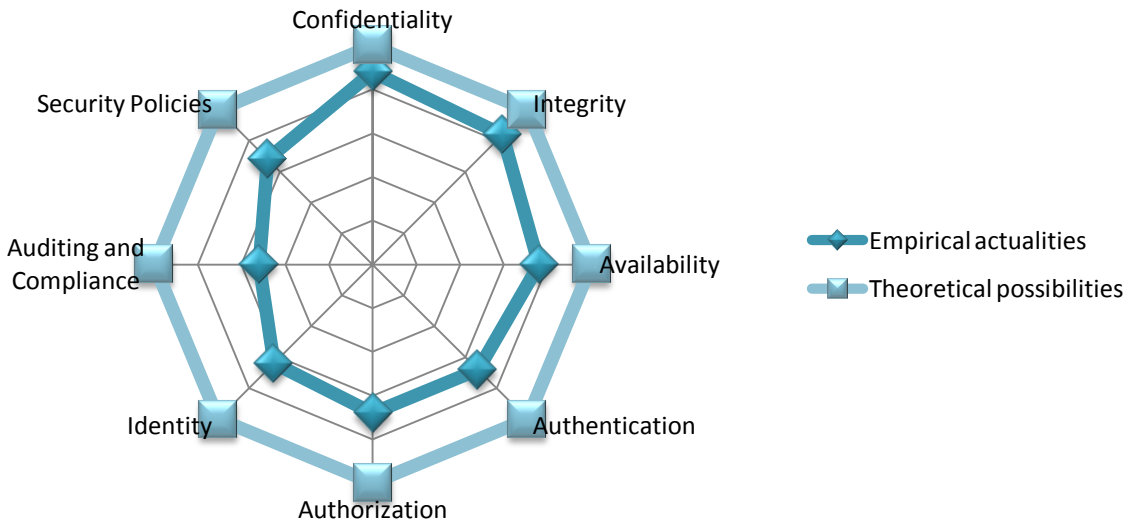


Confidentiality, Integrity and Availability were considered as the strong contenders for Data security. This is followed by Authentication, Authorization, Identity, Auditing and Compliance and finally Security policies.

Q9. To what extent are the aspects listed below relevant and critical for Knowledge security?

Knowledge is a fluid mix of framed experience, values, contextual information and expert insight that provide a framework for evaluating and incorporating new experiences and information (Davenport & Prusak, 1998). Knowledge can be classified into two types; Tacit, which is the un-codified knowledge in employee's heads, and Explicit, which is codified but easy to lose and is usually stored in specialized Knowledge Management System (KMS) (Tharun, 2005). This query determines to understand the significance of each of the security measures and concepts of SOA with respect to Knowledge security.

Criteria	**Empirical Answer (Rating x/5)**							
	P1	**P2**	**P3**	**P4**	**P5**	**P6**	**Avg.**	**Agreement**
Confidentiality	-	3	5	5	4	5	4.4	Strong
Integrity	-	2	5	5	4	5	4.2	Strong
Availability	-	2	5	3	4	5	3.8	Moderate
Authentication	-	4	4	4	2	3	3.4	Moderate
Authorization	-	4	4	4	2	3	3.4	Moderate
Identity	-	4	3	4	2	3	3.2	Moderate
Auditing and Compliance	-	1	3	3	1	5	2.6	Low
Security Policies	-	4	3	4	1	5	3.4	Moderate
Other	-	-	-	-	-	-	-	-
Info-graphics								

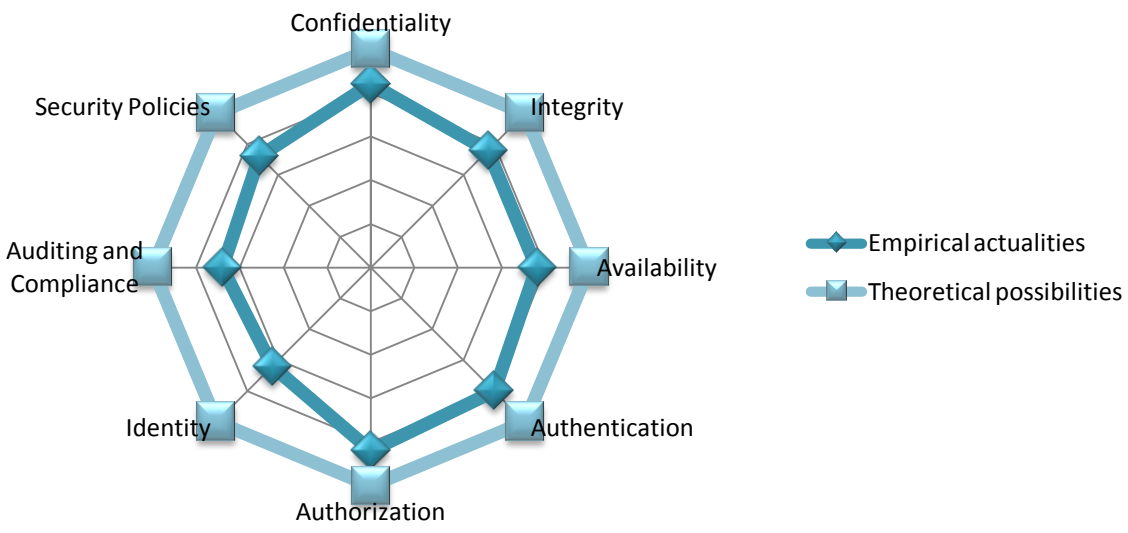


Confidentiality and Integrity were considered as the strong contenders for Knowledge security. This is followed by Availability Authentication, Authorization, Identity, Auditing and Compliance and finally Security Policies.

Q10. To what extent are the aspects listed below relevant and critical for Control security?

Control security refers to regulating access to data and administering processes in an information system. This query determines to understand the significance of each of the security measures and concepts of SOA with respect to Control security.

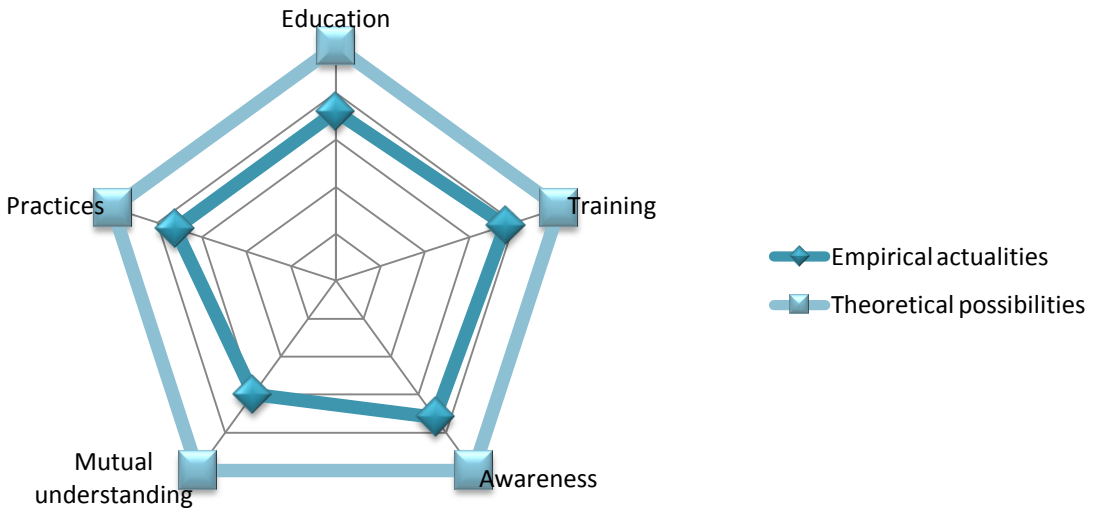
Criteria	Empirical Answer (Rating x/5)							
	P1	P2	P3	P4	P5	P6	Avg.	Agreement
Confidentiality	5	2	4	-	5	5	4.2	Strong
Integrity	4	2	4	-	4	5	3.8	Moderate
Availability	4	3	3	-	4	5	3.8	Moderate
Authentication	4	3	4	-	4	5	4	Strong
Authorization	5	3	4	-	4	5	4.2	Strong
Identity	4	2	3	-	2	5	3.2	Moderate
Auditing and Compliance	4	4	4	-	1	4	3.4	Moderate
Security Policies	5	4	4	-	1	4	3.6	Moderate
Other	-	-	-	-	-	-	-	-
Info-graphics								



Confidentiality, Authentication and Authorization were considered as the strong contenders for Control security. This is closely followed by Integrity, Availability, Security policies, Auditing and Compliance, and finally Identity. Most professionals perceive that Control security as an important informational task to enforce security measures and concepts.

Q11. To what extent are the capabilities listed below both necessary and efficient to promote Transport security?

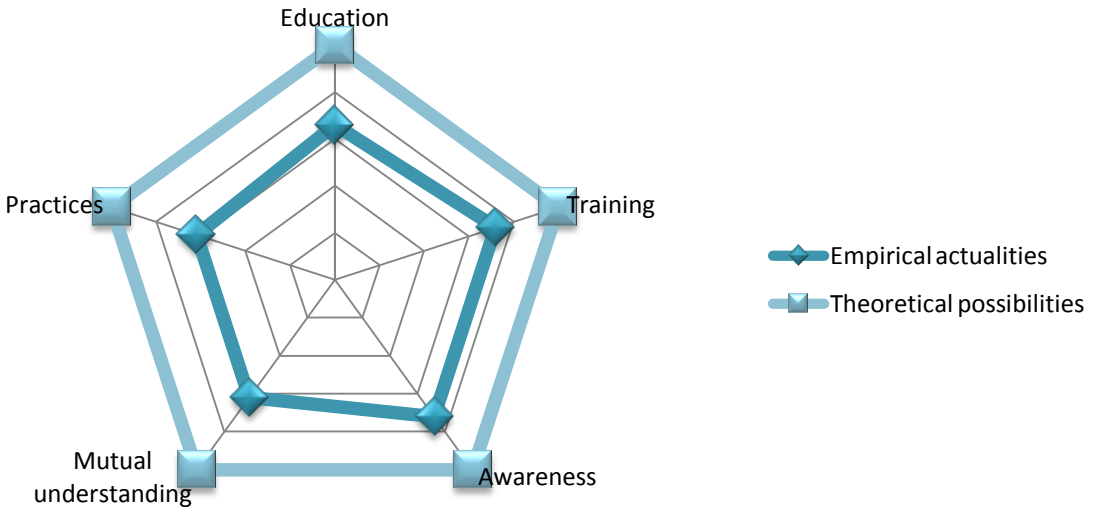
Criteria	Empirical Answer (Rating x/5)							
	P1	P2	P3	P4	P5	P6	Avg.	Agreement
Education	3	3	3	3	5	5	3.6	Moderate
Training	4	2	4	3	5	5	3.8	Moderate
Awareness	3	3	4	3	4	5	3.6	Moderate
Mutual understanding	3	3	3	2	4	3	3	Moderate
Practices	4	1	4	4	4	5	3.6	Moderate
Other	-	-	-	-	-	-	-	-
Info-graphics								



Most professionals have a mixed opinion about the capabilities required to promote Transport security but all the capabilities have a moderate rating.

Q12. To what extent are the capabilities listed below both necessary and efficient to promote Message security?

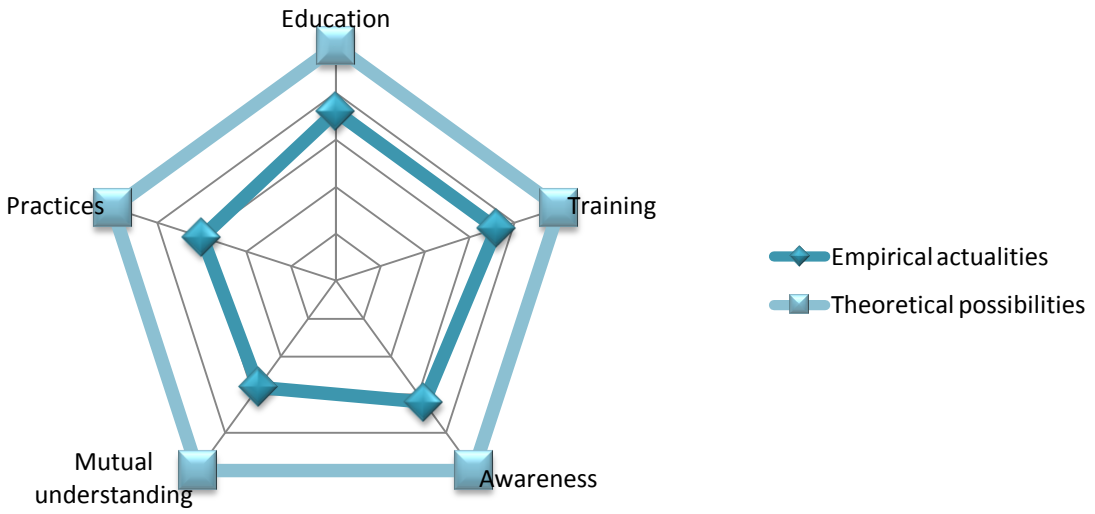
Criteria	Empirical Answer (Rating x/5)							
	P1	P2	P3	P4	P5	P6	Avg.	Agreement
Education	3	1	3	3	5	5	3.3	Moderate
Training	4	1	4	3	5	5	3.6	Moderate
Awareness	3	3	4	3	4	5	3.6	Moderate
Mutual understanding	3	3	4	2	3	4	3.1	Moderate
Practices	4	1	3	4	3	4	3.1	Moderate
Other	-	-	-	-	-	-	-	-
Info-graphics								



Most professionals have a mixed opinion about the capabilities required to promote Message security but all the capabilities have a moderate rating.

Q13. To what extent are the capabilities listed below both necessary and efficient to promote Application security?

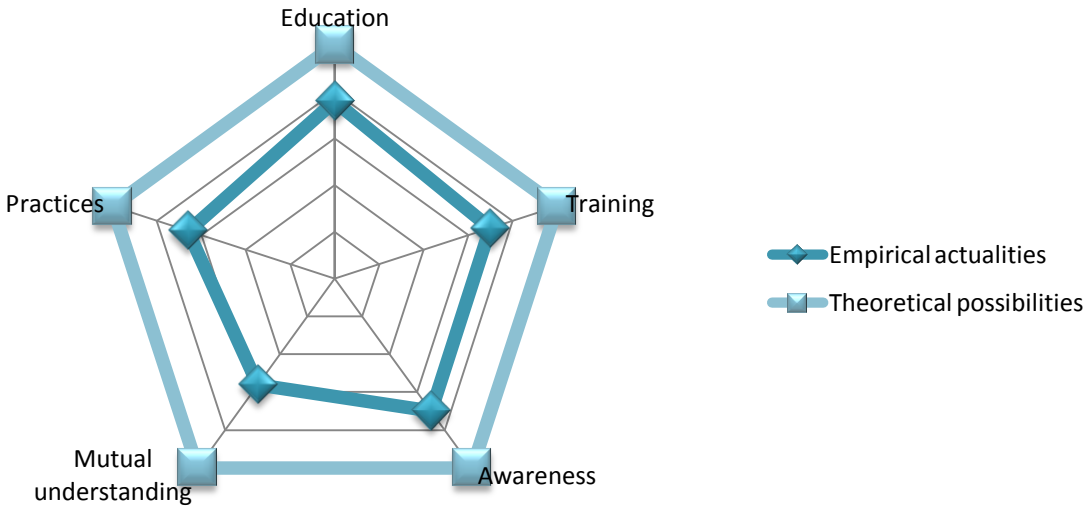
Criteria	Empirical Answer (Rating x/5)							
	P1	P2	P3	P4	P5	P6	Avg.	Agreement
Education	3	3	3	4	5	5	3.6	Moderate
Training	4	3	3	3	5	3	3.6	Moderate
Awareness	3	2	4	3	4	5	3.2	Moderate
Mutual understanding	4	2	2	3	3	3	2.8	Low
Practices	4	2	3	3	3	5	3	Moderate
Other	-	-	-	-	-	-	-	-
Info-graphics								



Most professionals have a mixed opinion about the capabilities required to promote Application security. Most of the capabilities have a moderate rating except for Mutual understanding which has a low rating.

Q14. To what extent are the capabilities listed below both necessary and efficient to promote Data security?

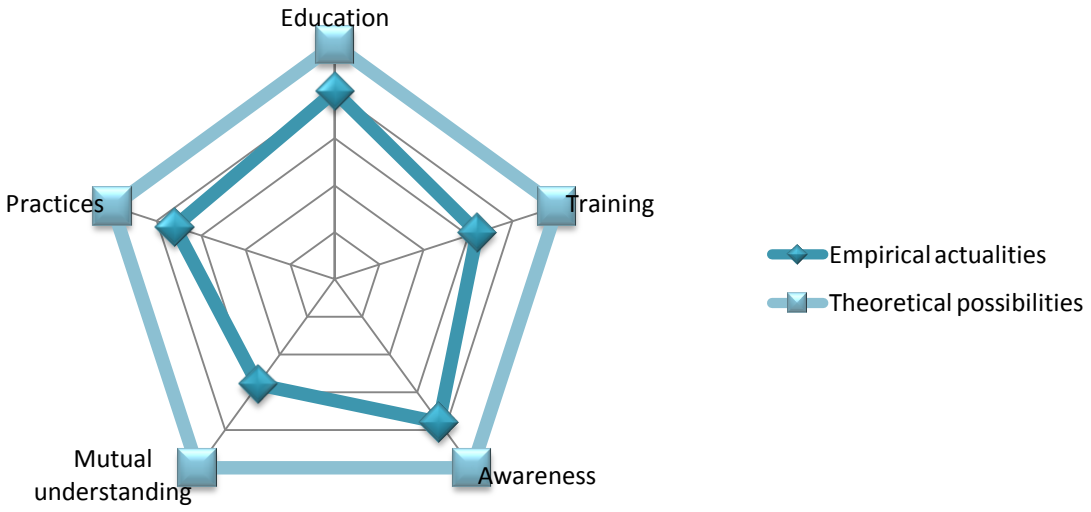
Criteria	Empirical Answer (Rating x/5)							
	P1	P2	P3	P4	P5	P6	Avg.	Agreement
Education	3	3	4	4	5	5	3.8	Moderate
Training	4	3	4	4	5	3	3.5	Moderate
Awareness	3	4	3	4	4	5	3.5	Moderate
Mutual understanding	4	4	4	1	4	5	2.8	Low
Practices	4	2	4	4	4	5	3.3	Moderate
Other	-	-	-	-	-	-	-	-
Info-graphics								



Most professionals have a mixed opinion about the capabilities required to promote Data security. Most of the capabilities have a moderate rating except for Mutual understanding which has a low rating.

Q15. To what extent are the capabilities listed below both necessary and efficient to promote Knowledge security?

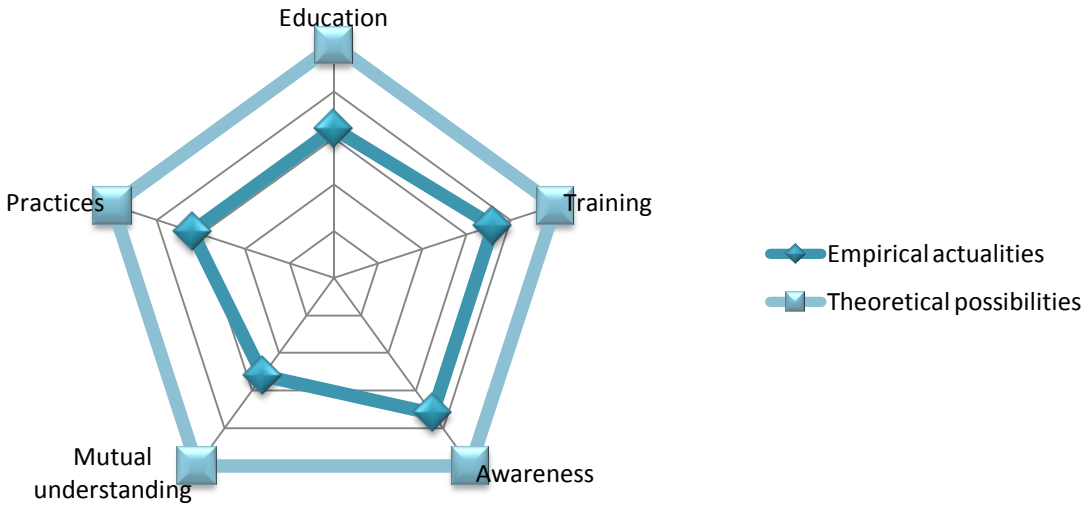
Criteria	Empirical Answer (Rating x/5)							
	P1	P2	P3	P4	P5	P6	Avg.	Agreement
Education	-	4	3	4	4	5	4	Strong
Training	-	3	4	3	3	3	3.2	Moderate
Awareness	-	3	4	4	3	5	3.8	Moderate
Mutual understanding	-	4	3	1	3	3	2.8	Low
Practices	-	3	4	3	3	5	3.6	Moderate
Other	-	-	-	-	-	-	-	-
Info-graphics								



Most professionals have a mixed opinion about the capabilities required to promote Knowledge security. Education is considered as a strong contender whilst Training, Awareness and Practices have a moderate rating. Mutual understanding is considered least favorable for knowledge security.

Q16. To what extent are the capabilities listed below both necessary and efficient to promote Control security?

Criteria	Empirical Answer (Rating x/5)							
	P1	P2	P3	P4	P5	P6	Avg.	Agreement
Education	3	1	3	-	4	5	3.2	Moderate
Training	4	1	4	-	4	5	3.6	Moderate
Awareness	3	3	4	-	3	5	3.6	Moderate
Mutual understanding	3	1	3	-	1	5	2.6	Low
Practices	4	2	4	-	1	5	3.2	Moderate
Other	-	-	-	-	-	-	-	-
Info-graphics								



Most professionals have a mixed opinion about the capabilities required to promote Control security. Most of the capabilities have a moderate rating except for Mutual understanding which has a low rating.

Q17. According to your opinion what are the three most crucial security issues necessary for SOA success?

According to various professionals, the most crucial security aspects necessary for SOA success are listed below;

Criteria	Empirical Answer					
	P1	P2	P3	P4	P5	P6
Confidentiality	√	-	√	√	√	√
Integrity	-	√	√	√	-	-
Availability	√	√	-	-	-	-
Authentication	√	-	-	-	-	√
Authorization	-	-	√	-	-	-
Security Policies	-	-	-	√	√	-
Identity	-	√	-	-	-	-
Education	-	-	-	-	-	√
Training	-	-	-	-	-	√

Q18. According to your experience, are any of the proposed requisites of SOA security (confidentiality, integrity, availability, etc) in conflict with others? Please write down these issues.

The interviewed professionals had varied views on this question. Some felt that the requisites of security are in fact complementary in nature. Some of the requisites which were considered as conflicting by some of the professionals are as follows;

- Confidentiality may conflict with transitive trust and circular dependency.
- Authentication and authorization may conflict with each other because of different security policies.
- Auditing and compliance may conflict with security policies.

These issues are discussed further in the next chapter (section 6.2.1).

6. Discussion

This chapter deals with comparison of the theoretical and empirical views based on which the partial conclusions are derived. The partial conclusions include a contextual understanding of the SOA environment and a clarification of relationships between the three dimensions of the integrated security model. This is followed by a section on proposals for future research.

6.1 Classification of similarities and differences behind the study

Before proceeding to the classification of results, we would like to clarify that SOA is a concept under development and therefore lacking a standard, unifying global definition. The CIA model was extended to meet the requirements of SOA. In the integration of SOA and extended CIA, it was expected to generate a multiplicity of interpretations

6.1.1 Queries contextual to the understanding of the SOA environment

Issues (Q1) Do you think it's a good strategy to insulate the direct contact between the service consumer and service provider?		
Theoretical Views	**Empirical Views**	**Similarities and differences between theory and reality**
According to Pajevski (2004), we can make use of a proxy service to insulate services from consumers and to split the service registry into public and private areas. All requests will have to go through the proxy service and the proxy gets authorization before forwarding any requests. Also, the messages will be checked for its format and any malicious content.	The answer to this query by all the interviewed professionals was unanimously 'Yes'. A separation of core services is always favorable in order to provide flexibility while maintaining system stability. It enables service loose coupling in a secure way whilst direct attacks are eliminated. It also helps in creating a layered approach to SOA security.	We can see that there is an excellent agreement between the theoretical and empirical views. The use of proxy services will help secure the SOA environment. The classical SOA model along with the proxy alternative provides a more flexible SOA environment. The load-balancing and QoS capabilities of the proxies also bestow the environment with greater stability.

Issues (Q2) To what extent do the following properties significantly express the property of Agility?		
Theoretical Views	**Empirical Views**	**Similarities and differences between theory and reality**
Agility requires loose coupling of services that participate in the composition of a business process. Agility also proposes loose coupling between both providers and consumers to the broker. Usually, the service consumer and provider do not have any knowledge about the composition of a process. By this way we give a clear answer to the uses of configuration. Agility also manifests itself into many other properties with respect to SOA (see page 21 and 22).	Most of the interviewed professionals have a varied view of Agility which is a core design principle of SOA. 'Flexibility' is determined as a strong match to Agility and 'Abstraction' as a low favored match. The other definitions of Agility have received mixed responses but are mostly positive.	Various authors in literature have defined agility in different terms. The empirical study points to 'Flexibility' as the closest match to define Agility. However, the above empirical answer is very limited because according to the actual trends, agility is a multi-dimensional concept.

Issues (Q3) To what extent do the following properties qualify to define the architectural integrity of SOA?		
Theoretical Views	**Empirical Views**	**Similarities and differences between theory and reality**
The properties and design principles of SOA have been elegantly discussed by various authors like Artus (2006), Jossutis (2007) and Erl (2008) in their respective books. However, there is a conflicting interpretation of architectural integrity. This conflict arrives from the SOA concept and not with respect to security. However, there are those that exclude reusability from the architectural integrity of SOA. According to study of Kingkarn (2008), the idea of SOA accommodating the	Agility or Loose coupling and Visible or Discoverable are perceived to be the foundational properties of SOA architecture. The other properties like Consistency, Statelessness, Reusability, Granularity and Composability etc. must always be in harmony with the foundational ones.	It is not surprising that Agility or Loose coupling is perceived as a key property of SOA as it manifests into many other properties, but most professionals agree that all the properties collectively define the architectural integrity of SOA.

principle of reusability was rejected because it creates dependencies that go against the requisites of loose coupling. The available redundancy is just the solution of loosely coupling.		

Issues (Q4) To what extent are the following approaches relevant to the characteristics of an architecture that addresses the use of security?		
Theoretical Views	**Empirical Views**	**Similarities and differences between theory and reality**
There are several design solutions of SOA, but none of these implementations have taken security into consideration (i.e. security as an intrinsic aspect of the architecture). Most of these design solutions depend on external security measures such as encryption, firewalls, pad-locking etc. Furthermore, some of the concerning design solutions do not satisfy the architectural integrity of SOA or posses corresponding principles which are conflicting in nature.	Though there are several design solutions of SOA, most professionals believe that Web-service Architecture (WSA), Enterprise Integration Architecture (EIA) and Enterprise Service Architecture (ESA) inherently address the use of security. The other design solutions like Agility driven SOA, ESB and Reusability driven SOA are considered more susceptible to be lacking security.	There seems to be a conflict between theory and reality in this case. Most professionals perceive some of the implementations of SOA i.e. Web-service Architecture (WSA), Enterprise Information Architecture (EIA) and Enterprise Service Architecture (ESA) as secure but in reality this is not the case. Also, as per our study the proper design solutions of SOA must be based on ESB or Agility driven SOA.

6.1.2 Queries based on the relationship between the domain of Informational tasks and the domain of security measures and concepts

Issues (Q5 – Q10) To what extent are the aspects listed below relevant and critical for the different Informational tasks i.e. Transport security, Message security, Application security, Data security, Knowledge security and Control security?		
Theoretical Views	**Empirical Views**	**Similarities and differences between theory and reality**
Confidentiality can be ensured by the use of encryption techniques. Integrity can be enforced using a set of rules or constraints. Availability ensures that information and supporting systems being usable and accessible on a timely basis. Authorization allows the identified entity to access a resource. Authentication is the process of establishing or confirming the identity of a user. Identity is an essential attribute required to authenticate a user. Auditing helps us to detect security vulnerabilities and respond with suitable measures, whilst compliance is the state of being in accordance with established guidelines, specifications and legislation. Security policies help to maintain and address all	Confidentiality, Integrity and Availability were considered as the strong contenders for Transport security. Confidentiality and Integrity were considered as the strong contenders for Message security. Confidentiality, Integrity, Availability, Authentication, Authorization and Identity were considered as the strong contenders for Application security. This is closely followed by Security policies, Auditing and Compliance. Confidentiality, Integrity and Availability were considered as the strong contenders for Data security. Confidentiality and Integrity were considered as the strong contenders for Knowledge security. Confidentiality, Authentication and Authorization were considered as the strong contenders for Control security. This is closely	Confidentiality and Integrity are considered to be vital for enforcing security at all levels. This is closely followed by Availability, Authentication and Authorization. Finally other measures like Identity, Auditing and Compliance and Security Policies are considered. Most professionals perceive that Application security and Control security should most likely include these security measures and concepts.

aspects of information security.	followed by Integrity, Availability and Security policies.	

6.1.3 Queries based on the relationship between the domain of informational tasks and the domain of security capabilities

Issues (Q11 – Q16) To what extent are the aspects listed below relevant and critical for the various Informational tasks i.e. Transport security, Message security, Application security, Data security, Knowledge security and Control security?		
Theoretical Views	**Empirical Views**	**Similarities and differences between theory and reality**
The security capabilities represent the support level provided by the solution to the corresponding security measure and concept v/s the Information task.	Most professionals have a mixed opinion about the capabilities required to promote security for the various informational tasks. Mutual understanding which has a low rating when it comes to application security, data security, knowledge security and control security. Education is considered to be a strong contender to promote knowledge security.	Most professionals have a mixed opinion on this issue but all of them agreed that these capabilities help to secure the various informational tasks.

6.1.4 Queries based on the relationship between the domain of security measures and concepts, and domain of security capabilities

Issues (Q17) According to your opinion what are the three most crucial security issues necessary for SOA success?		
Theoretical Views	**Empirical Views**	**Similarities and differences between theory and reality**
Confidentiality, Integrity and Availability (CIA) are the core security requirements of any information system. SOA environments dictate additional security requirements such as Authorization, Authentication, Identity, Security Policies, Auditing and Compliance etc.	Confidentiality, Integrity, Availability, Authentication and Security policies were considered as the prime contenders for SOA success. The other aspects included Authorization, Identity, Education and Training.	A fruitful answer could have been provided if a larger number of professionals would have been interviewed. Insofar, it can be said that security measures, concepts and capabilities are required for an attractive, collaborative and secure SOA environment.

6.2 Proposals for future research

6.2.1 Conflicting interpretations on some security issues

It would be interesting to undertake a future study concentrating and focusing on some conflicts that have been pointed out by respondents taking part in the empirical study. For instance, in the query 18 (Q18), there are at least three critical aspects of such conflicts namely;

- Confidentiality may conflict with transitive trust and circular dependency.
- Authentication and authorization may conflict with each other because of different security policies.
- Auditing and compliance may conflict with security policies.

6.2.2 Clarifying the architectural integrity of SOA

Architectural integrity is the concept that defines the foundation and consistency of a particular SOA architecture. As we have demonstrated in the query 3 (Q3), such a foundation is given based on a few significant principles that together support each other. However, in the foundation of SOA we have two principles that are in conflict with each other. They are the principle of Agility and the principle

of Reusability. Accordingly, the principle of Agility promotes the ideas of flexibility, adaptability, resilience etc. but not the economics of maintenance of such environment. The idea of reusability on the other hand promotes the economics and maintenance of services, but this is against the requisites of agility. Therefore, theoretically this concept cannot co-exist in the same architectural foundation. However, this study takes into account the uses of security to state the requirements of architectural integrity. It considers the uses of security principles of Confidentiality, Integrity, Availability, etc. The question is what architectural foundation of SOA is best for security?

According to the theoretical views of the SOA concept there are two interpretations of architectural integrity of SOA. The first interpretation covers both the uses of agility and the uses of reusability. However, the second interpretation excludes from the architectural integrity the concept of reusability because it goes against the requisites of loosely coupling in the composition of services as well as the configuration of a SOA environment (Kingkarn, 2008). The importance of architectural integrity has been further emphasized in Appendix B (Dynamics in the Architectural integrity of SOA).

Flexibility is one of the most critical aspects of Agility. It refers to the capability to achieve success in different ways (Alberts & Hayes, 2005). As stated earlier, flexibility can be accomplished by making allowable design changes i.e. either in terms of introducing modules or modifications or by withdrawing existing modules.

6.2.3 Security perspective to the Service-oriented life-cycle

The SOA life-cycle model is intended to illustrate the relationships and dependencies between the various stages which are applied within a SOA project. There are various life-cycle models defined by various organizations. The IBM Foundation life-cycle model is one of the most notable models used in the industry today (see Appendix B). This model consists of the following life-cycle phases (IBM 2007);

- **Model** - Modeling is the process of capturing the business design based on the understanding from business requirements and objectives.

- **Assemble** - The business design is used to communicate the business objectives to the respective organization that will assemble the information system to implement the design.

- **Deploy** - The deploy phase of the life cycle includes a combination of creating the hosting environment for the applications and the deployment tasks of those applications.

- **Manage** - The manage phase includes the tasks and technologies used to manage and monitor the services and business processes that are deployed to the production environment.

This life-cycle can also be extended to security which encompasses all aspects of the aforementioned life-cycle. There are various stakeholders in any organization who define, manage and monitor security issues during the execution of the service-oriented life-cycle.

This life-cycle can be included as an additional dimension (fourth dimension) to the integrated SOA security model, but it needs to be separately verified for compatibility with all the aspects of security. Also, the life-cycle model has to be controlled and monitored within the constraints of SOA Governance.

7. Conclusion

This final section of the thesis deals with summarizing the contents of this thesis i.e. creation of an integrated security model for the management of SOA, along with its constituent dimensions which focuses on a secure, collaborative and attractive service environment.

7.1 Towards a sound theory of SOA security

The study intends to answer the following problem statement;

What concepts and principles should define a secure collaborative and attractive service environment?

The above problem statement was decomposed to provide the basis for an explanatory theory that promotes the understanding of the following issues;

- Why is security such a crucial issue for the service environment?
- How can the security of a collaborative service environment improved trough the application of CIA concept?
- Are the principles and concepts of CIA triad enough, or must they be updated first and then integrated to the SOA concept as well as to the enterprise of SOA Governance?

7.1.1 Why is security such a crucial issue for the service environment?

According to the study, a SOA environment cannot be attractive if the aspects of security are excluded from the architecture. We also have a clear agreement between theoretical and empirical views that the providers of such an environment should be not directly accessed by customers. The study provides a modified configuration of a SOA environment by the use of a proxy service. Furthermore, there are relatively accepted correspondences between the theoretical and empirical views with respect to interpretations of Agility as a necessary presupposition for the creation of an agile attractive SOA environment.

There is a conflicting view of architectural integrity i.e. the principles covered by the SOA architecture. This conflict can be explained in terms of two conflicting interests i.e. conflict between agility and reusability as well as the conflict between the adequacies of optimal implementation options. In the first case at least theoretically, agility promotes the requisites of responsiveness, flexibility, innovation, adaptation etc. but is against questions of economy because proposes the existence of redundancy. Reusability promotes economy but is against agility because it eliminates redundancy and creates interdependencies (Kingkarn, 2008).

7.1.2 How can the security of a collaborative service environment improved trough the application of CIA concept?

As the study indicates, there is a great agreement between the theoretical and empirical views with respect to the foundational principles of security namely Confidentiality, Integrity and Availability. Accordingly an attractive, collaborative environment must be designed and maintained with respect to such foundational requisites. Furthermore, the extended requisites of security such as Authentication, Authorization etc. also provide a strong agreement between theoretical and empirical views. There is a relatively acceptable otherwise a moderate agreement between the theoretical and empirical views for principles such as Auditing and Compliance and Security policies. Also, one can note that some cases of security where the uses of Availability have a moderate rather than strong agreement. However, this can be perceived as a result of ignorance rather than a result of knowledge. So, with respect to the necessary and sufficient capabilities for promoting the attractiveness and collaborativeness of SOA environment we can state the following;

Firstly, every aspect of security capabilities covered in this study has a moderate agreement between the theoretical and empirical views. This moderation we believe can be explained in terms of lack of experience with the concepts of SOA related security. Also, the uses of mutual understanding have a low agreement. However, this is a topic for further research to provide a better understanding of the relationships between the various aspects for service security and the requisites of capabilities to maintain and further develop such environments.

The relationships between security principles, requisites and capabilities related to the creation, maintenance and evaluation of a SOA environment has provided varied interpretations about what aspects of security are critical. The most critical may be seen as Confidentiality and Integrity; all the other aspects have a diversified opinion. Furthermore the capabilities that are crucial to this aspect of security have been given in terms of education and training. Lastly, my expectations here were to find a stronger agreement between theoretical and empirical views. However, because such an agreement is missing, it has to be considered as an impending case for further research.

7.1.3 Are the principles and concepts of CIA triad enough, or must they be updated first and then integrated to the SOA concept as well as to the enterprise of SOA Governance?

This study demonstrates that there are several aspects of security not covered by the foundational principles of security. These security requirements of SOA include Authentication, Authorization, Identity, Auditing, Compliance and Security Policies along with the primary security requisites Confidentiality, Integrity and Availability. It is important to satisfy all these requirements in order to secure a SOA environment comprehensively. However, as we have stated above in the section above the empirical views of security are consistent but disintegrated and hence they do not have equal value.

This argument is based on the theory where the principles of SOA and CIA should create the foundation upon which an integrated SOA architecture should dictate, guide and manage the requisites for comprehensibility, mutual understanding and attractiveness of a so called service collaborative environment.

The SOA security model proposed in this study (section 4.1) proposes a solution by addressing these security requirements. Additionally, the integrated model of secure-governed environment enabled with proxy services (section 3.5) illustrates an integrated framework for SOA Governance which facilitates the governance and management of the environment. This model also illustrates the relationships between the three dimensions of the SOA security model for maintaining a secure service environment. Another notable feature is the use of proxy services to insulate services from consumers and to split the service registry into public and private areas. The proxy services to an extent helps eliminate direct attacks and also augment the service with enhanced capabilities like load-balancing, quality of service (QoS), etc. In summary, it can be concluded that the service environment agrees with the security requisites of SOA.

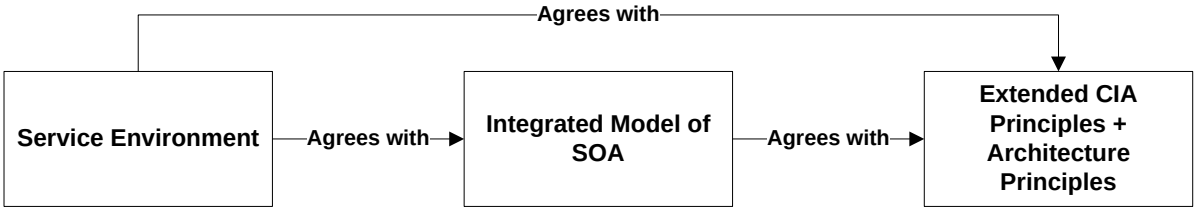


Figure 17 – Towards a sound theory of SOA Security

The main purpose of this thesis is to create an integrated model of security which can define a secure, attractive and collaborative SOA-environment. Also, in order to create and verify this model the managerial and governance aspects of SOA also needs to be considered as it plays a cardinal role in shaping the SOA business environment.

7.2 The relationship between SOA security measures, Informational tasks and capabilities

An integrated model for SOA security consisting of three dimensions i.e. security measures and concepts, informational tasks and capabilities.

- The first dimension of the SOA security model consists of explicit security measures and concepts such as: Confidentiality, Integrity, Availability, Authentication, Authorization, Identity, Auditing and Compliance and Security Policies, etc.

- The second dimension of the SOA security model consists of informational tasks such as: Transport security, Message security, Application security, Data security, Knowledge security, Control security, etc. Each of the components of the first dimension (tuple of security measures and concepts) can be correlated with the components of this dimension.

- The last dimension of the SOA Security model deals with the requisites of capabilities such as: Education, Training, Awareness, Mutual understanding, Practices etc. Each of the components of this dimension (tuple of security capabilities) can be used to empower the second dimension (tuple of informational tasks).

8. References

Books, Journals and Papers

1. Josuttis, N. M. (2007). [Chapter 2, 3]. In *SOA in Practice*. Cambridge, Paris: O'Reilly.
2. Kingkarn K. (2008). *An Integrated Model for SOA Governance*. Unpublished master's thesis, IT University of Göteborg. Retrieved January 10, 2009, from http://gupea.ub.gu.se/dspace/handle/2077/10495
3. *An Introduction to Computer Security*: The NIST Handbook. Washington, DC: National Institute of Standards and Technology, Technology Administration. Washington, DC: U.S. Department of Commerce, 1995, p. 11.
4. Rescher, N. (1979). *Cognitive Systematization: A Systems-Theoretic Approach to a Coherent Theory of Knowledge*. Blackwell.
5. Bubenko, J. (1978). Validity and Verification aspects of Information Modeling, 3rd International Conference of Very Large Databases.
6. Ramarao, K., & Prasad, C. (2008). SOA requires new approaches to security. *In SOA Security* (pp. 11-12) [Introduction]. Greenwich: Manning.
7. Erl, T. (2008). [Chapter 4]. In *SOA Principles of Service Design*. Prentice Hall.
8. Metzler, D., & Davis, P. (2002, March 1). *Employing a Mixed-mode Qualitative Research method prior to conducting Quantitative Research*. Retrieved from http://www.icis.dk/ICIS_papers/A1_5_5.pdf
9. Alberts, D., & Hayes, R. (2005, April). Chapter 8: Agility. *In Power to the Edge: Command and Control in the Information Age*. CCRP Publication Series. Retrieved from http://www.dodccrp.org/files/Alberts_Power.pdf
10. Henderson, R., & Clark, K. (1990). Architectural Innovation: *The Reconfiguration of Existing Product Technologies and the Failure of Established Firms*. Administrative Science Quarterly, Vol. 35.
11. Generally Accepted System Security Principles (GASSP) Version 2.0. (1999, June). *Generally Accepted System Security Principles*. Retrieved from http://www.theiia.org/download.cfm?file=365
12. Synder, L., & Leffler, C. (2005). *Ethics Manual*. American College of Physicians.
13. Department of Health and Human Services (2005). The Common Rule, Protection of Human Subjects. Code of Federal Regulations Title 45, Part 46.102 (d).
14. Dawson, C. (2002). Chapter 2. *In Practical Research Methods.* Oxford: How To Books Ltd.

15. NSTISS. (1994, June 20). *National Training Standard For Information Systems Security (INFOSEC) Professionals* (Rep. No. 4011). Retrieved from www.cnss.gov/Assets/pdf/nstissi_4011.pdf
16. NSTISS. (1992, November 16). *National Training Standard For Information Systems Security (INFOSEC) Professionals* (Rep. No. 501). Retrieved from http://www.dtic.mil/cgi-bin/ GetTRDoc?AD=ADA404177&Location=U2&doc=GetTRDoc.pdf
17. Davenport, T., & Prusak, L. (1998). *Introduction*. In Working Kowledge. Harvard Business School Press.
18. Solotruk M & Kristofic M (1980), Increasing the Degree of Information System Integration and Developing an Integrated Information System, North Holland Publishing Company.
19. IBM. (2007, November). Understanding SOA Security - Design and Implementation. Retrieved from http://www.redbooks.ibm.com/abstracts/sg247310.html

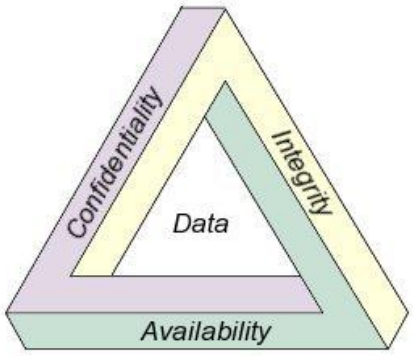
Electronic Documents

1. Service-oriented architecture. (n.d.). Wikipedia. Retrieved January 22, 2009, from http://en.wikipedia.org/wiki/Service-oriented_architecture
2. Hao, He. (2003, September 30). What Is Service-Oriented Architecture? In xml.com. Retrieved January 22, 2009, from http://www.xml.com/pub/a/ws/2003/09/30/soa.html
3. OASIS. (n.d.). Wikipedia. Retrieved January 24, 2009, from http://en.wikipedia.org/wiki/Organization_for_the_Advancement_of_Structured_Information_Standards
4. NIST. (n.d.). Wikipedia. Retrieved January 24, 2009, from http://en.wikipedia.org/wiki/National_Institute_of_Standards_and_Technology
5. Information assurance. (n.d.). Wikipedia. Retrieved January 26, 2009, from http://en.wikipedia.org/wiki/Information_assurance
6. Regeringskansli. (n.d.). Retrieved April 12, 2009, from Regeringskansliet Web site: http://www.regeringen.se/sb/d/9509/a/95411
7. Search facilities. (n.d.). LIBRIS [About LIBRIS]. Retrieved January 28, 2009, from http://www.libris.kb.se/english/search.jsp
8. Larsson, C. (n.d.). LIBRIS Progress Report 1998. Retrieved January 28, 2009, from http://elag.kb.nl/elag/index.html?http://elag.kb.nl/elag99/reports/libris.html

9. Arsanjani, A. (2004, November 9). Service-Oriented Architecture: A conceptual model. In *Service-oriented modeling and architecture*. Retrieved February 2, 2009, from http://www.ibm.com/developerworks/webservices/library/ws-soa-design1/
10. UCSF. (2008). Prevention and Public Health Group. In *Triangulation.* Retrieved February 27, 2009, from http://www.igh.org/triangulation/
11. Artus, D. (2006, February 17). *SOA realization: Service design principles*. Retrieved February 4, 2009, from http://www.ibm.com/developerworks/webservices/library/ws-soa-design/
12. Mitra, T. (n.d.). Layered architecture view. In *Documenting software architecture, Part 3: Develop the architecture overview*. Retrieved June 27, 2008, from IBM Web site: http://www.ibm.com/developerworks/library/ar-archdoc3/index.html
13. McAllister, N. (n.d.). *Identity's role in SOA*. Retrieved September 3, 2004, from http://www.infoworld.com/article/04/09/03/36FEidentitynetsoa_1.html
14. Duke University. (2001, August). Risk of confidentiality breach can make HIV patients shy from treatment. Message posted to http://www.scienceblog.com/community/older/2001/B/200111935.html
15. Pulier, E., & Taylor, H. (2005, November). Solutions to SOA Security. Retrieved March 12, 2009, from http://www.developer.com/design/article.php/3607471
16. Peterson, G. (2008, February 9). Security in SOA - It's the Car, Not the Garage. Message posted to http://www.soamag.com/I15/0208-2.pdf
17. Manoj, C. (2005, March). Bracing for the compliance storm. Message posted to http://www.networkmagazineindia.com/200503/vendorvoice01.shtml
18. Maclinovsky, A. (2007, November 15). A Formal SOA Security Model. Message posted to http://blogs.sun.com/RealSOA/entry/soa_security_model
19. Maclinovsky, A. (2007, November 15). Security Model Details. Message posted to http://blogs.sun.com/RealSOA/entry/security_model_details
20. Pajevski, M. (2004). *A Security Model For Service-Oriented Architectures* [Data file]. Retrieved March 10, 2009, from NASA Web site: http://www.oasis-open.org/committees/download.php/17573/06-04-00008.000.pdf
21. Nagaratnam, N., Nadalin, A., Mostow, J., & Muppidi, S. (2007, September). SOA Security Reference Model. STSC CrossTalk. Retrieved March 11, 2009, from http://www.stsc.hill.af.mil/crosstalk/2007/09/0709NagaratnamNadalinMostowMuppidi.html

22. Youmans, J. (2008). Methods of SOA Security Engineering and Certification [Data file]. Retrieved March 15, 2009, from Concurrent Technologies Corporation Web site: http://www.jeff-youmans.com/PPT/Youmans%20DoDIIS%20WorldWide%2008.ppt
23. Tharun, K. (2005, October 7). Managing knowledge security . Business Line. Retrieved from http://www.thehindubusinessline.com/2005/10/07/stories/2005100700151100.htm

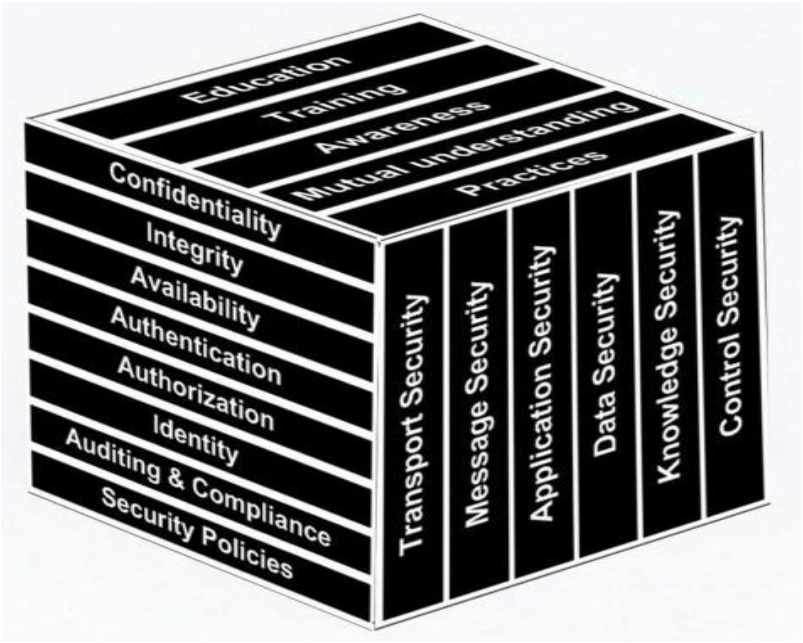
Appendix A – Questionnaire: Inquiring the Issues of SOA Security



The purpose of my study is to create an integrated model of security aiming to support the definition of a secure, and attractive collaborative SOA-environment. Therefore we try to clarify empirically the following question:

What concepts, principles and practices should define a secure and attractive collaborative service environment?

The question is directly related to the conceptual model below that describes the most crucial issues of security and their relationships.



An Integrated Model for SOA Security

- The first dimension of the SOA security model consists of explicit security measures and concepts such as: Confidentiality, Integrity, Availability, Authentication, Authorization, Identity, Auditing and Compliance, Security Policies, etc.

- The second dimension of the SOA security model consists of informational tasks such as: Transport security, Message security, Application security, Data security, Knowledge security, Control security, etc.

- The last dimension of the SOA Security model deals with the requisites of capabilities such as: Education, Training, Awareness, etc.

Instructions for answering the Questionnaire

The rating scale for answering the questionnaire is described below;

Rating Scale:

0 – Not Important

1 – Marginally Important

2 – Moderately Important

3 – Extremely Important

4 – Blockbuster

*Kindly **select** the suitable answer by clicking on the check-box. Also, justify using textual answers as and when required.*

Q1. Do you think it's a good strategy to insulate the direct contact between service consumer and service provider?

Some models of SOA security makes use a proxy service to insulate services from consumers and to split the service registry into public and private areas. The proxy services to an extent helps eliminate direct attacks and also augment the service with enhanced capabilities like load-balancing, quality of service (QoS), etc.

☐ Yes
☐ No
Because…….

Q2. To what extent do the following properties significantly express the property of Agility?

Agility is one of the key property or design principle of SOA. Agility also manifests itself into many other properties of SOA and it is important to identify to what extent these properties are aligned with respect to the property of Agility.

Quickness	☐	☐	☐	☐	☐
Robustness	☐	☐	☐	☐	☐
Abstraction	☐	☐	☐	☐	☐
Flexibility	☐	☐	☐	☐	☐
Innovativeness	☐	☐	☐	☐	☐
Adaptively	☐	☐	☐	☐	☐
Resilience	☐	☐	☐	☐	☐
Continuity	☐	☐	☐	☐	☐

Other……...

Q3. To what extent do the following properties qualify to define the architectural integrity of SOA?

This question deals with properties or the design principles of SOA The understanding of these properties is vital as they play a role in shaping the SOA environment. The SOA environment follows the system of principles that together defines the architectural integrity of SOA. But, this does not exclude the situation where the system of principles is viewed inconsistent and therefore insufficient for determining the desirability of architectural integrity.

Agility or Loose coupling	☐	☐	☐	☐	☐
Visible or Discoverable	☐	☐	☐	☐	☐
Consistency	☐	☐	☐	☐	☐
Statelessness	☐	☐	☐	☐	☐
Reusability	☐	☐	☐	☐	☐
Granularity or Composability	☐	☐	☐	☐	☐
Other……...					

Q4. To what extent are the following approaches relevant to the characteristics of an architecture that addresses the use of security?

The approaches listed below are the various design solutions of SOA. Though these approaches don't take into security as a critical requirement, their success is greatly influenced by the requisites of security.

Web-service Architecture (WSA)	☐	☐	☐	☐	☐
Enterprise Integration Architecture (EIA)	☐	☐	☐	☐	☐
Enterprise Service Bus (ESB)	☐	☐	☐	☐	☐
Enterprise Service Architecture (ESA)	☐	☐	☐	☐	☐
Reusability driven SOA	☐	☐	☐	☐	☐
Agility driven SOA	☐	☐	☐	☐	☐
Other……...					

Q5. To what extent are the aspects listed below relevant and critical for Transport security?

Transport security is essential when the information is in transit i.e. when information is exchanged between the constituent services in SOA. This deals with the relationship between the security measures and concepts of SOA and the requisites for Transport security.

Confidentiality	☐	☐	☐	☐	☐
Integrity	☐	☐	☐	☐	☐
Availability	☐	☐	☐	☐	☐
Authentication	☐	☐	☐	☐	☐
Authorization	☐	☐	☐	☐	☐
Identity	☐	☐	☐	☐	☐
Auditing and Compliance	☐	☐	☐	☐	☐
Security Policies	☐	☐	☐	☐	☐

Other……..

Q6. To what extent are the aspects listed below relevant and critical for Message security?

The whole idea of SOA is based on messages exchanged between services. In the case of Message security all the information related to security is encapsulated in the message. The individual messages (request/response) are routed between service consumers, providers and intermediaries. This query determines to understand the significance of each of the security measures and concepts of SOA with respect to Message security.

Confidentiality	☐	☐	☐	☐	☐
Integrity	☐	☐	☐	☐	☐
Availability	☐	☐	☐	☐	☐
Authentication	☐	☐	☐	☐	☐
Authorization	☐	☐	☐	☐	☐
Identity	☐	☐	☐	☐	☐
Auditing and Compliance	☐	☐	☐	☐	☐
Security Policies	☐	☐	☐	☐	☐

Other……..

Q7. To what extent are the aspects listed below relevant and critical for Application security?

Information processing (Application) security must be protected from external threats. This could involve security mechanisms that are directly coupled with the application logic. Security measures and concepts minimize the likelihood that hackers will be able to manipulate applications and access, modify, or delete sensitive data. This query deals with the significance of each of the security measures and concepts of SOA with respect to Application security.

Confidentiality	☐	☐	☐	☐	☐
Integrity	☐	☐	☐	☐	☐
Availability	☐	☐	☐	☐	☐
Authentication	☐	☐	☐	☐	☐
Authorization	☐	☐	☐	☐	☐
Identity	☐	☐	☐	☐	☐
Auditing and Compliance	☐	☐	☐	☐	☐
Security Policies	☐	☐	☐	☐	☐
Other…….……..					

Q8. To what extent are the aspects listed below relevant and critical for Data security?

Data security involves regulating access and ensuring that the data is safe from corruption or loss. It also helps in ensuring privacy and protecting personal information.

Confidentiality	☐	☐	☐	☐	☐
Integrity	☐	☐	☐	☐	☐
Availability	☐	☐	☐	☐	☐
Authentication	☐	☐	☐	☐	☐
Authorization	☐	☐	☐	☐	☐
Identity	☐	☐	☐	☐	☐
Auditing and Compliance	☐	☐	☐	☐	☐
Security Policies	☐	☐	☐	☐	☐
Other…….……..					

Q9. To what extent are the aspects listed below relevant and critical for Knowledge security?

Knowledge is a fluid mix of framed experience, values, contextual information and expert insight that provide a framework for evaluating and incorporating new experiences and information. It is necessary to protect the documents and artifacts in the Knowledge Management System by using access control mechanisms, intrusion prevention mechanisms and using intellectual property (IP) protection. This query deals with the significance of each of the security measures and concepts of SOA with respect to Knowledge security.

Confidentiality	☐	☐	☐	☐	☐
Integrity	☐	☐	☐	☐	☐
Availability	☐	☐	☐	☐	☐
Authentication	☐	☐	☐	☐	☐
Authorization	☐	☐	☐	☐	☐
Identity	☐	☐	☐	☐	☐
Auditing and Compliance	☐	☐	☐	☐	☐
Security Policies	☐	☐	☐	☐	☐
Other……..					

Q10. To what extent are the aspects listed below relevant and critical for Control security?

Control security refers to regulating access to data and administering processes in an information system and/or information network. This query deals with the significance of each of the security measures and concepts of SOA with respect to Control security.

Confidentiality	☐	☐	☐	☐	☐
Integrity	☐	☐	☐	☐	☐
Availability	☐	☐	☐	☐	☐
Authentication	☐	☐	☐	☐	☐
Authorization	☐	☐	☐	☐	☐
Identity	☐	☐	☐	☐	☐
Auditing and Compliance	☐	☐	☐	☐	☐
Security Policies	☐	☐	☐	☐	☐
Other…….					

Q11. To what extent are the capabilities listed below both necessary and efficient to promote Transport security?

Education	☐	☐	☐	☐	☐
Training	☐	☐	☐	☐	☐
Awareness	☐	☐	☐	☐	☐
Mutual understanding	☐	☐	☐	☐	☐
Practices	☐	☐	☐	☐	☐

Other……...

Q12. To what extent are the capabilities listed below both necessary and efficient to promote Message security?

Education	☐	☐	☐	☐	☐
Training	☐	☐	☐	☐	☐
Awareness	☐	☐	☐	☐	☐
Mutual understanding	☐	☐	☐	☐	☐
Practices	☐	☐	☐	☐	☐

Other……...

Q13. To what extent are the capabilities listed below both necessary and efficient to promote Application security?

Education	☐	☐	☐	☐	☐
Training	☐	☐	☐	☐	☐
Awareness	☐	☐	☐	☐	☐
Mutual understanding	☐	☐	☐	☐	☐
Practices	☐	☐	☐	☐	☐

Other……...

Q14. To what extent are the capabilities listed below both necessary and efficient to promote Data security?

Education	☐	☐	☐	☐	☐
Training	☐	☐	☐	☐	☐
Awareness	☐	☐	☐	☐	☐
Mutual understanding	☐	☐	☐	☐	☐
Practices	☐	☐	☐	☐	☐

Other……...

Q15. To what extent are the capabilities listed below both necessary and efficient to promote Knowledge security?

Education	☐	☐	☐	☐	☐
Training	☐	☐	☐	☐	☐
Awareness	☐	☐	☐	☐	☐
Mutual understanding	☐	☐	☐	☐	☐
Practices	☐	☐	☐	☐	☐

Other……...

Q16. To what extent are the capabilities listed below both necessary and efficient to promote Control security?

Education	☐	☐	☐	☐	☐
Training	☐	☐	☐	☐	☐
Awareness	☐	☐	☐	☐	☐
Mutual understanding	☐	☐	☐	☐	☐
Practices	☐	☐	☐	☐	☐

Other……...

Q17. According to your opinion what are the three most crucial security issues necessary for SOA success?

1. …….
2. …….
3. …….

Q18. According to your experience are any of the proposed requisites of SOA security (confidentiality, integrity, availability, etc) in conflict with others? Please write down these issues

……
……
……
……

Q19. Please describe your occupation/role in your organization?

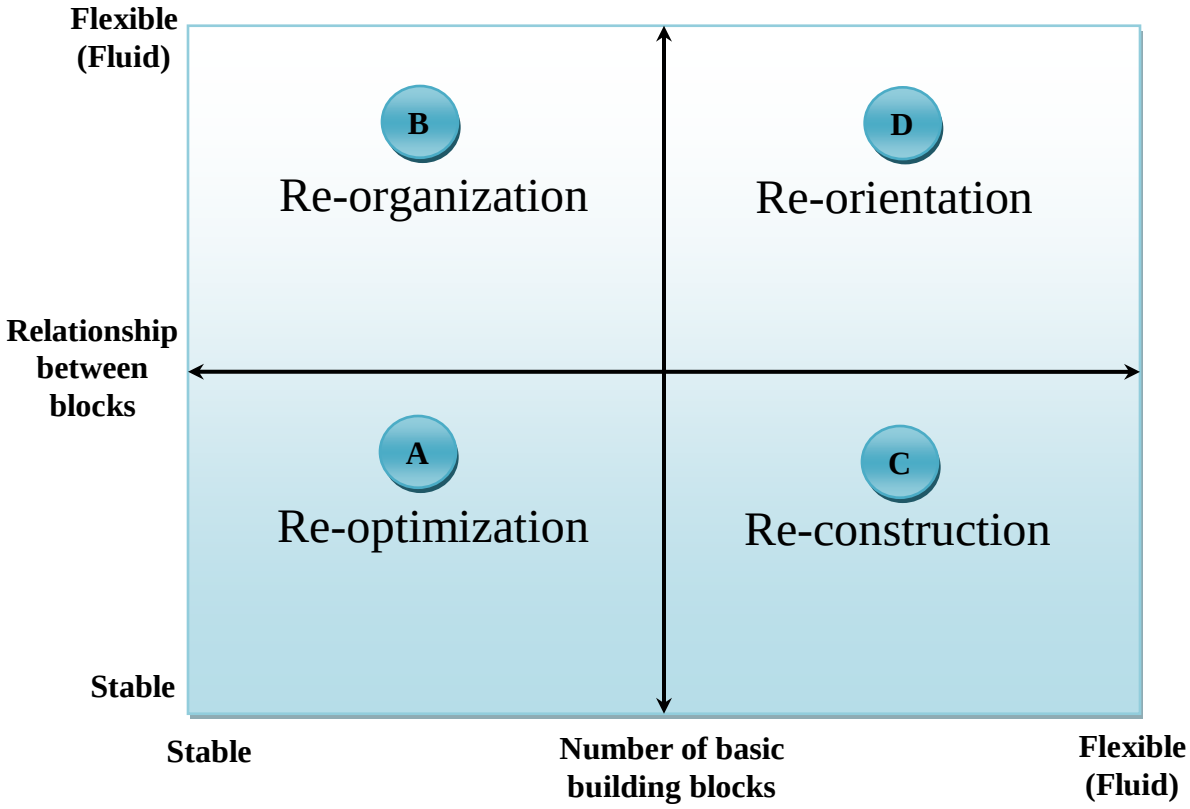
☐ Business Manager
☐ CEO
☐ CTO
☐ Programmer
☐ Educator
☐ User
Other……..

Q20. Please describe in what segment of business does your organization belong?

☐ Industry
☐ Public Service
☐ Business
☐ Trust-board
Other……

Appendix B – Dynamics in the Architectural Integrity of SOA

The dynamics of the architectural integrity of SOA can be illustrated by the diagram below.



Dynamics in the Architectural Integrity of SOA[23]

The architectural integrity of SOA can vary between the two extremes i.e. stable to unstable (flexible). In the state A, changes to the architectural design and pattern are not allowed. This means that the constituent modules and connections cannot be changed. In state B, the relationships between the modules are unstable as it allows several connections between each of the constituent modules. In state C, the architectural integrity is defined in terms of stable relationships. Any changes are allowed only within the constraints of the constituent modules. Finally in the case of state D, the unstable relationships lead to a new design which would result in a change of architectural identity.

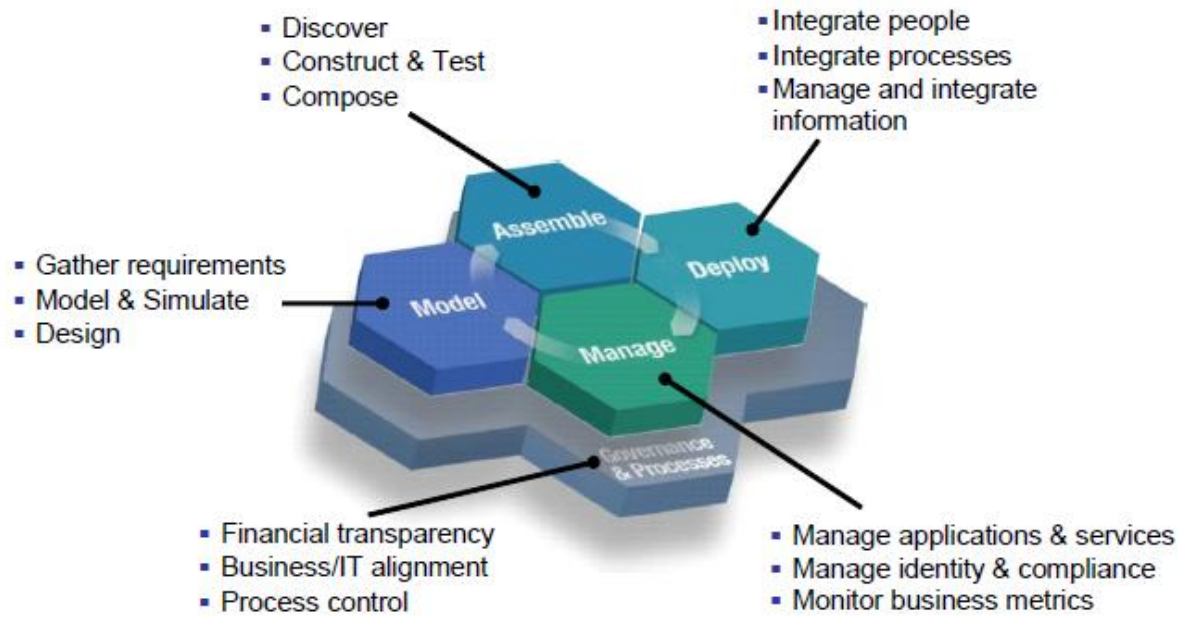
[23] Henderson & Clark (1990), Solotruk & Kristofic (1980)

Appendix C – SOA Foundation Life-cycle (IBM, 2007)

IBM clients have indicated that they think of SOA in terms of a life cycle. As seen in the figure below, the IBM SOA Foundation includes the following life cycle phases:

- Model
- Assemble
- Deploy
- Manage

There are a couple of key points to consider about the SOA life cycle. First, the SOA life cycle phases apply to all SOA projects. Second, the activities in any part of the SOA life cycle can vary in scale and the level of tooling used depending on the stage of adoption.



IBM SOA Foundation Life-cycle

Model

Modeling is the process of capturing the business design from an understanding of business requirements and objectives. The business requirements are translated into a specification of business processes, goals, and assumptions for creating a model of the business. Many businesses do not go through a formal modeling exercise. In some case, businesses that do perform modeling use primitive techniques, such as drawing the design in Visio® or using text documents.

Capturing the business design using a sophisticated approach that includes the use of specialized tooling lets you perform what-if scenarios with various parameters that the business might experience. The process can then be simulated using those parameters to predict the effect that process will have on the business and IT systems. If the achieved results do not match the business objectives, then the process definition can be refined.

The model also captures key performance indicators that are important measurements of your business, such as business metrics. For example, these measurements can include a measure of the new accounts that you have opened in a given month. These key performance indicators are built into the assembly of the application. In addition, you can monitor the indicators in production, capturing critical data to measure if the objectives are being met.

Assemble

The business design is used to communicate the business objectives to the IT organization that will assemble the information system to implement the design. The enterprise architect works closely with the business analyst to convert the business design into a set of business process definitions, as well as activities used to derive the required services from the activity definitions. The enterprise architect and business analyst work with the software architect to fully develop the design of the services.

While you are resolving the design and implementation of the modeled business processes and services, you should perform a search of existing artifacts and applications to find components that meet the design requirements. Some applications will fit perfectly. Some applications will have to be refactored, and some applications will have to be augmented to meet the design requirements.

These existing assets should be rendered as services for assembly into composite applications. Any new services required by the business design must be created. Software developers should use the SOA programming model to create these new services.

And finally, the assemble phase includes applying a set of policies and conditions to control how your applications operate in the production runtime environment. For example, these policies and conditions include business and government regulations. In addition, the assemble phase includes critical operational characteristics, such as packaging deployment artifacts, localization constraints, resource dependency, integrity control, and access protection.

Deploy

The deploy phase of the life cycle includes a combination of creating the hosting environment for the applications and the deployment tasks of those applications. This includes resolving the application's resource dependencies, operational conditions, capacity requirements, and integrity and access constraints.

A number of concerns are relevant to construction of the hosting environment, including the presence of the already existing hosting infrastructure supporting applications and pre-existing services. Beyond that, you must consider appropriate platform offerings for hosting the user interaction logic, business process flows, business services, access services, and information logic.

Manage

The manage phase includes the tasks, technology, and software used to manage and monitor the services and business processes that are deployed to the production runtime environment. Monitoring is a critical part of ensuring the underlying IT systems and applications are up and running to maintain service availability requirements.

Monitoring includes these activities:

- Monitoring performance of service requests and timeliness of service responses

- Maintaining problem logs to detect failures in various services and system components, as well as localizing failures and restoring the operational state of the system

Managing the system also involves performing routine maintenance, administering and securing applications, resources, and users, and predicting future capacity growth to ensure that resources are available when the demands of the business warrant using them. The security domain includes topics, such as authentication, single sign-on, authorization, federated identity management, and user provisioning.

The manage phase also includes managing the business model, tuning the operational environment to meet the business objectives expressed in the business design, and measuring success or failure to meet those objectives. SOA is distinguished from other styles of enterprise architecture by its correlation between the business design and the software that implements that design, and it is distinguished by its use of policy to express the operational requirements of the business services and processes that codify the business design. The manage phase of the life cycle is directly responsible for ensuring those policies are being enforced and for relating issues with that enforcement back to the business design.

Governance

SOA Governance is critical to the success of any SOA project. Governance helps clients extend the planned SOA across the enterprise in a controlled manner. SOA Governance has four core objectives or challenges:

- Establish decision rights.
- Define high value business services.
- Manage the life cycle of your assets.
- Measure effectiveness.