Department of Informatics

Enterprise Architecture

&

Security Architecture Development

Master Thesis in Informatics, 15p

Submitted: June 2011

Authors: Shahram Jalaliniya
Farzaneh Fakhredin

Supervisor: Markus Lahtinen

Examiners: Agneta Olerup
Hans Lundin

Lund University
Informatics

Title:	Enterprise Architecture & Security Architecture Development
Authors:	© Shahram Jalaliniya
	© Farzaneh Fakhredin
Publisher:	Department of Informatics, Lund University
Supervisor:	Markus Lahtinen
Examiners:	Agneta Olerup
	Hans Lundin
Year of publication:	2011
Type of thesis:	Master Thesis
Language:	English
Key words:	Enterprise Architecture (EA), Security Architecture (SA)

Abstract

By increasing importance of information for enterprises and appearing new forms of threats such as cyber-attacks, information warfare, and terrorism, information security has become one of the most significant concerns of enterprises. On the other hand, Enterprise Architecture (EA) as a holistic approach tries to address main concerns of enterprises; therefore, the frameworks and methods of EA have considered security issues. However, EA frameworks follow different strategies to address security concerns, but most of the EA frameworks and methods have accepted the Security Architecture (SA) term as a holistic approach to security concern. Nevertheless, there are some frameworks and methods to develop SA independent of EA. The present study seeks to clarify relationship between EA and SA by describing relevant examples from the literature review and addressing SA in different EA frameworks. The study aims to classify and evaluate different SA development strategies based on previous works and interviewing EA experts. According to the findings of this research, developing SA independent of EA, using EA knowledge in developing SA, using EA artifacts in to develop SA, and developing SA as a part of EA are the main strategies of SA development. Also, integrating SA and EA development leads to increasing effectiveness and efficiency of SA development.

Acknowledgments

We thank those who have reviewed our works and given us insightful comments. It is the pleasure to thanks our supervisor, Markus Lahtinen, and all of the interviewees who had enriched our work with their valuable input and ongoing support.

We also would like to express our gratitude to Swedish Armed Forces and Mr. Ross W Tsagalidis as our industry supervisor for his guidance and willingness to provide time for counseling and completing of our master thesis. Thank you

I would like to acknowledge my parents who have made available their supports in a number of ways. Also I would like to show my deepest gratitude to my wife Banafsheh and my daughter Sheida for their support during the long hours and lost weekends required to write this thesis.

Shahram Jalaliniya
Lund University, June 2011

First and foremost, I would like to have a special thanks to Shahram Jalaliniya, whose patience, encouragement, guidance and support from the initial to the final part of thesis enabled me to develop an understanding of the subject. And my deepest gratitude and love to my wonderful parents who always pushed me up and helped me to keep my feet on the ground and reaching for the stars!

Farzaneh Fakhredin
Lund University, June 2011

Contents

List of Figures

List of Tables

1 Introduction and Background

1.1 Introduction

By increasing pressure of competition, firms have to be able to change their products and services to satisfy their customers. Also, they have to reduce price of products and services to retain customers, so that using new technologies to automate processes is inevitable. On the other hand, pace of change in requirements of customers, technology, regulation, and culture is increasing all the time. Indeed, today, the art of managing business and technological changes is a crucial skill for enterprises. To manage change of a complex object like enterprise, it should be possible to anticipate consequences of changes, and without a big picture of enterprise, we cannot track related elements of enterprise. This big picture of enterprise which depicts enterprise elements and relationships between these elements called Enterprise Architecture. (Zachman, 1997)

Enterprise Architecture (EA) is a holistic image of enterprise which describes enterprise from both business and technology viewpoints by several models. When business managers look at the enterprise, they see strategies, goals, business processes, roles and responsibilities of people, and other resources which should be aligned to produce products or services of enterprise. Also from the IT points of view, enterprise is a collection of data that should be processed by applications which are installed on the IT infrastructures to help business processes. EA is a picture of enterprise which describes not only the strategies, business processes, roles, and responsibilities of enterprise, but also how the strategies are determining organization units, how business processes are realizing strategies, and who is responsible for business processes. EA also illustrates an integrated blueprint of information, applications, and IT infrastructures. This blueprint explains which information is needed to perform business processes by organizational units and how applications process data to produce and distribute information. In addition, EA demonstrates how IT infrastructures (servers, network, storage, and etc.) support applications to provide informational services to the business.

Since EA models cover most of enterprise elements and their relationships, EA could be used as a knowledgebase in decision making process of enterprise. In fact, EA models can help decision makers understand current situation, analyze different alternatives, and evaluate consequences of each alternative. For example, if a bank decides to provide a new service to the customers, the decision makers should be aware of current organizational and IT capacities. They need to know which business processes will be involved to provide new service and which applications will support the business processes. Also the planners have to be able to estimate the new IT capacity to support

this change. Based on this information, they could define different alternatives such as providing new services by current business processes, employees and IT infrastructures, extending business and IT capacities, or outsourcing some parts of business process or IT services. In this example, EA models could be used to identify related elements of enterprise and analyze cost-benefits of different alternatives.

Enterprise Architecture (EA), firstly introduced by Zachman (1987) as a structure to describe information systems architecture, but he extended his classifying approach to the whole enterprise. Now, many enterprises are using EA approach to manage change, align IT with business, reduce costs, decrease complexity, improve information quality, and manage stakeholders' concerns. In addition, the main focuses of EA programs have been integration, Service Oriented Architecture, and security. (Spewak et al., 1994; Schekkerman, 2004; Schekkerman, 2005; Infosys, 2009)

Also EA has been considered as a fundamental approach to plan IT especially in public and defense sectors (Finkelstein, 2006; Hjort, 2009). In fact, military organizations such as Department of Defense of US started using EA to improve interoperability and integrity of military systems in joint and combined operations; however, they extended EA application from war fighting processes to the business processes. Now, several Enterprise Architecture Frameworks are being used in defense sector such as DoDAF by US Department of Defense, NAF by NATO, DNDAF by Canadian military forces, and MODAF by UK and Sweden.

On the other hand, the role of information in creating competitive advantage (Porter et al, 1985) has given rise to increasing the importance of information security concerns. So that several information security standards, models and frameworks have been developed to support enterprises against probable threats. Today, the widespread use of the Internet led to signifying new types of threats such as information warfare, thus enterprises are more vulnerable to cyber-attacks. Indeed, anyone can launch information attack and damage critical infrastructures such as banks and economic centers. As an illustration, the OMB (2010) official reports shows increasing security incidents from 5503 incidents in 2006 to 41776 incidents in 2010. In fact, changing form of the threats and merging IT with business have increased complexity of information security and need for a holistic approach to manage complexity.

By expanding use of EA approach in enterprises and increasing need for a holistic view to the security, Security Architecture concept was created. The architectural approach can help enterprises classify main elements of information security from different points of view and decrease complexity of relationships between information security and other elements of enterprise. Moreover, EA logical structure as a holistic perspective on

addressing key concerns of stakeholders could be applied to manage security concerns. Also EA as the repository of all sub-architectures such as business, system, data, and technology architectures can encompass security architecture, but security architecture has been considered differently in EA frameworks. Some of the EA frameworks such as DoDAF have not addressed security architecture explicitly and just tried to cover security concerns in the background of their architectural products. Some others such as DNDAF and E2AF have considered security architecture explicitly as a viewpoint. Furthermore, MODAF framework as a customized instance of DoDAF, has addressed security architecture explicitly and defined some goals and objectives for security architecture, but there is no viewpoint, architectural product, or method for security architecture in MODAF. With regard to increasing importance of security for enterprises, it is crucial for enterprises to choose the most effective strategy for developing security architecture.

1.2 Problem statement

The enterprises manage their information security by using different models, standards, and frameworks. On the other hand, EA as a holistic view tries to integrate different viewpoints and focuses such as business, system, technology and security. But different EA frameworks have not a clear and unified approach to the information security architecture, and enterprises follow different strategies to develop security architecture. Different strategies could be generated out of different contexts because security architecture is a complex concept and could not be defined universally, and each organization can define security architecture based on its requirements and context (Amer et al., 2008). But the problem is that it is not clear which strategies could be selected and which general points should be considered to choose a strategy and develop SA. As an important step in academic research on information security architecture, this thesis aims to review and classify different strategies of information security architecture development, evaluate consequences of each strategy, and extract general points of different strategies to help other enterprises develop their SA. The result of this research is important for enterprises who decided to develop information security architecture. Some of these enterprises have developed EA models, so they want to know how they could customize their EA framework to support information security architecture development; how EA artifacts could be used to develop information security architecture; also which parts of EA should be integrated with information security architecture. For instance, the Swedish Armed Forces, as the initiator of this research, have developed EA models based on MODAF. Now, they decided to develop security architecture, but it is not clear what different strategies they could follow, and which strategy could be appropriate with their context and expectations.

1.3 Research question

Since security architecture is one of the architectural descriptions of enterprise the main question of this thesis is:

> *Q1: What are different strategies to develop Security Architecture in relation with Enterprise Architecture?*

After identifying different alternative strategies to develop Security Architecture, it is crucial to evaluate different strategies in terms of effectiveness, cost, and time of SA development. Therefore the second question of this research is defined as below:

> *Q2: What are the advantages and drawbacks of strategies of security architecture development?*

Since Enterprise Architecture is characterized by EA framework, and EA framework illustrates main concerns of stakeholders, it is important to evaluate way of addressing security as a main concern of enterprises in different EA frameworks. Reviewing strategies of different EA frameworks to develop security architecture could help enterprises select appropriate EA framework, and reuse experiences of other frameworks to upgrade their EA framework. Hence, our last research question is defined as follows:

> *Q3: How EA frameworks can support enterprises to develop security architecture?*

1.4 Research purposes

The purpose of this research is to identify, classify and evaluate different strategies of security architecture development in relation with EA.

1.5 Limitation and delimitation

Since each organization selects limited strategies to develop security architecture, it is not possible to observe implications of selecting all strategies in a unique context; therefore, this research will review different strategies of security architecture development based on previous published works and interviewing EA experts. In other words, all of the advantages and drawbacks of each strategy will not be observed necessarily in a particular case. Also, because of different definitions of security architecture in EA frameworks, the results of this research could be applied to each framework differently appropriate with its terminology and components.

2 Literature Review

Regarding research questions, the main goals of literature review is defined as reviewing literature of key concepts in the research such as enterprise architecture, security architecture, and their relationships. Also, to answer third research question, we will review famous EA frameworks to discover how security concerns are addressed by each framework.

2.1 Enterprise Architecture

To review the enterprise architecture literature in the following section, a brief history of enterprise architecture is explained because history of EA shows when EA has been invented and by comparing EA and SA history we can analyze historical dependencies of EA and SA. Moreover, the importance of enterprise architecture is discussed, and drivers of EA are reviewed. EA drivers show stakeholders' expectations of EA which reveals importance of security related expectations of implementing EA. Then we will review the most referred definitions of enterprise architecture; however, the goal of this research is not to compare different definitions of enterprise architecture. Like other approaches, EA implementing has its own challenges and problems which are discussed in this section. EA challenges would be useful to understand how EA has succeeded in achieving defined goals.

2.1.1 History of Enterprise Architecture

The concept of Enterprise Architecture has been introduced in 1987 when John Zachman (1987) published his suggested information systems architecture framework in IBM Systems Journal. However, in 1970 Dewey Walker, as the team leader of Zachman in IBM, defined information architecture concept in Business System Planning (BSP) method (Internet 1). In the BSP methodology, information architecture matrix shows how functions manipulate data by Creating, Reading, Updating, or Deleting data-subjects. Information architecture matrix, which is also called CRUD matrix, just describes the data and function interactions, but Zachman matrix, in a higher level of abstraction, covers data, function, people, location, time, and motivation. Zachman, in his published article, discussed how his suggested framework would help managing complexity of distributed information systems. Also he republished a revision of his previous framework as Enterprise Architecture Framework in 1992 (Sowa & Zachman, 1992). In fact, the Zachman's paper was considered seriously by IS/IT researchers and professionals and attracted lots of attention. The reason is that Zachman contributed his framework based on his experiences in IBM, as one of the pioneer IT companies in the

world. Besides, his framework was the first holistic structure to merge business concerns with IT and align IT and Business discourses.

The Zachman framework was an abstract structure which explained way of thinking to the enterprise information, and he did not proposed any methodology for developing EA artifacts. So that in 1994, Steven Spewak (1994) published his book about a methodology to develop architectural blueprints based on Zachman Framework. His developed methodology, Enterprise Architecture Planning, is one of the main references of next EA methods (Figure 2.1). The concepts of As-Is and To-Be Architecture which have been used by further frameworks and methods firstly introduced by Spewak in EAP methodology.

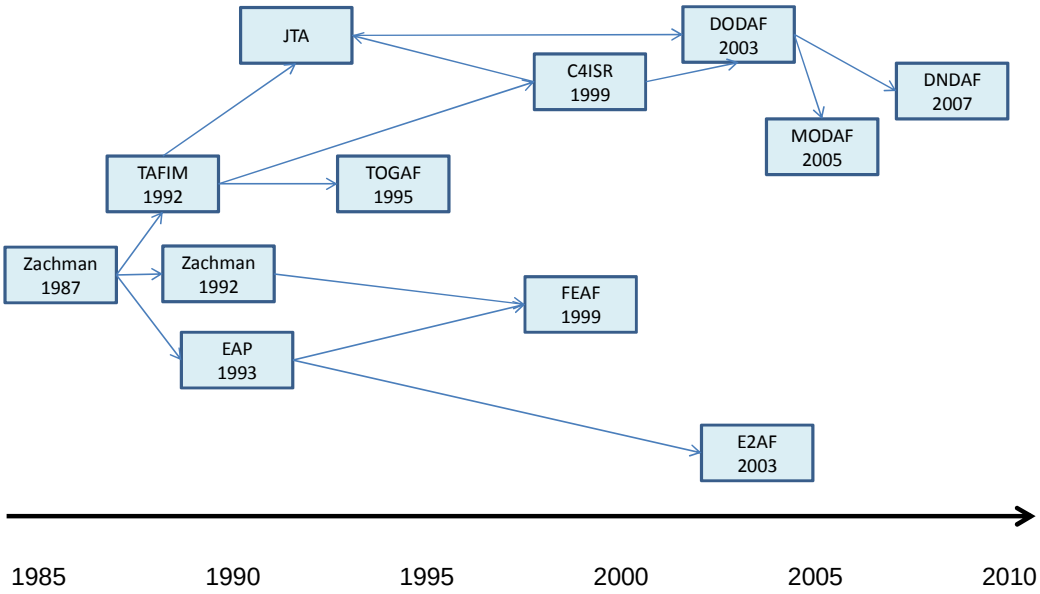

Figure 2.1. History of Enterprise Architecture development (Schekkerman, 2004)

In 1990, the Department of Defense of US issued the interoperability problems in Gulf War, and they found EA approach as a solution for this problem. Therefore, development of Technical Architecture Framework for Information Management (TAFIM) started in 1992. TAFIM was the first organizational practice in using EA approach. Now TAFIM is retired, and Department of Defense uses Joint Technical Architecture (JTA), as a technical standard, to manage interoperability of operation, data, and systems. In fact, Department of Defense of US has played a major part in developing and operationalizing EA approach. Also, Open Group, as a consortium of companies which aims to establish vendor-neutral IT standards, developed first version of The Open Group Architecture Framework (TOGAF) based on TAFIM in 1995. (Mitre, 2004)

The Congress of US passed Clinger-Cohen Act (1996) which legislate that all of the Federal Agencies had to develop and maintain their IT architectures to increase efficiency and effectiveness of IT investment. According to this act, Chief Information Officer (CIO) of each Federal agency was responsible to develop a 5-year IT strategic plan and provide their performance report annually. The Clinger-Cohen act was the most significant driver for developing EA in US, and several EA program were conducted by Federal departments and agencies such as National Institute of Standards and Technology, Department of Treasury, Department of Transportation, and Department of Energy. (Clinger-Cohen act, 1996)

In 1996, US Department of Defense developed first version of Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance (C4ISR) Architecture Framework to direct subcontractors and agencies on how document system architectures to increase interoperability and comparability between architectures. The C4ISR Framework has been completed and changed to Department of Defense Architecture Framework in 2003. The version 2.0 of DoDAF has been published in 2009. C4ISR was the first framework which developed a meta-model for EA products and artifacts called Core Architecture Data Model (CADM).

After announcing Clinger-Cohen Act and increasing demand for Enterprise Architecture frameworks and methods, in 1999, CIO Council developed Federal Enterprise Architecture Framework (FEAF) in order to optimize IT investment by promotion of common federal processes and applications, sharing information among federal agencies, and improvement interoperability between federal agencies (CIO Council, 1999). The most important contribution of FEAF to the EA community was the reference model concept which is described in the FEAF security section.

In 2005, Ministry of Defense of UK developed an EA framework based on DoDAF version 1.0. Now, some of external partners such as BAE Systems, Thales, Lockheed Martin, Boeing and Serco as well as MOD are using MODAF. Also recently, Swedish Armed Forces developed their EA artifacts based on MODAF (Internet 2). In addition, some other military EA frameworks such as E2AF (Netherland defense framework in 2003), and DNDAF (Department of National Defence and the Canadian Forces in 2007) developed based on DoDAF. Figure 2.1 illustrates a graphical history of EA development and influences of each framework on others.

As the history of EA shows, the concept of EA has been firstly created and developed among the EA frameworks. Moreover, US government and defense sectors have played an important part in operationalizing EA as a holistic approach to IT planning.

2.1.2 Drivers for Enterprise Architecture

Enterprise Architecture is a holistic blueprint of the enterprise components such as strategies, business processes, applications, data, and IT infrastructures regarding past, present and future of the enterprise. Therefore, if we consider EA as a city plan, the most important benefits of this plan will be in constructing, integrating, and maintaining the components of enterprise (Niemann, 2006). For example, when an enterprise decides to develop a new application, the process models of enterprise architecture could help to define main functional requirements of the application. Also system architecture blueprints could be used to understand the relationships of new application with other applications, and the infrastructure specifications and standards could be useful in defining technical restrictions of new application. Moreover, when a business process needs to change out of changing strategies or changing requirements of customers, application and data architectures can help enterprise discover related processes, applications, and databases. Therefore, impacts of the change could be evaluated, and enterprise managers can plan for required activities to manage and implement the change.

Zachman (2008) describes need for enterprise architecture blueprints to manage change by an example of building architecture. If we do not have the architecture and design blueprints of a building, and we want to change something in the building, we will have three choices: First, we can accept the risk of the change that might lead to destroying the building completely. Second option is trying to develop architectural blueprints by searching in documents and reverse engineering that would be costly and time-consuming. Third alternative is giving up and constructing a new building. In the case of enterprise, if we want to change an enterprise element such as an application or business process, the first option would have high risk, second one would be a long and expensive process, and the third alternative will not be possible.

According to the survey by Schekkerman (2005), the most significant reasons for developing EA in order of importance are as follows:

1. *"Supports decision making"***:** as mentioned in the introduction section, EA models could be used in analyzing decision consequences and different alternatives.
2. *"Delivers roadmaps for change":* EA as an integrated repository of business and IT blueprints helps enterprises track technological and business changes and identify enterprise elements which would be affected by the changes (Sowa & Zachman, 1992).
3. *"Manages IT portfolio":* the main goal of IT portfolio management is maximizing benefits of IT investment. EA as a holistic and integrated IT plan helps IT department define, prioritize and control IT development projects and activities.

Also, due to defining reusable software services and components in EA; cost and time of systems development will decrease and IT services will be delivered shortly at lower cost.

4. *"Managing complexity":* in the information age, most of the business processes are performing based on IT. Furthermore, globalization resulted in changing market borders, and even local businesses have to compete globally. EA can be used to classify business and IT concerns without fear of disintegration which would contribute simplicity of managing business and IT issues. For example, if a global company decides to establish new branch in another country, some of the local rules such as tax regulations have to be observed. The business rule models of EA could be used to analyze and integrate global and local rules which would reduce complexity of issue.
5. *"Supports systems development":* system developers are one of the main stakeholders of EA. In fact, EA blueprints play a crucial part in large scale systems development. EA business models could be used in requirements analysis of system development, data architecture can be used to define information flow between systems, and technology architecture determine software development technologies such as programming language, standards, case tools, and etc.
6. *"Supports business and IT budget prioritization":* the transition architecture as one of the most important deliverables of EA, describes projects and actions which should follow to transition from current state to the desired situation (Fatolahi & Jalalinia, 2003). The technical and managerial precedents and budget of projects are defined in the transition plan.
7. *"Delivers insight and overview of business and IT":* EA as a big picture of enterprise defines IT requirements of the business. Also, as a result of transparency in interrelations of IT and business and creating common language to communicate, the IT goals and business goals will be aligned.

Enterprises usually decide to approach EA when they face challenge. In Schekkerman's survey, enterprises plan EA for the following issues: "ERP implementation, business change, mergers/acquisition, Application renewal, transformation roadmap, business-IT alignment, infrastructure renewal, and legacy transformation" (Schekkerman, 2005). For example, when an enterprise decided to implement ERP system, first of all a vendor or product have to be chosen. In order to select ERP system the business strategies and business model of enterprise should be analyzed to find the most appropriate ERP product. Also by investigating the current IT architecture, enterprise could estimate costs and benefits of different alternatives. Moreover, in order to implement ERP system, To-Be business architecture has to be designed. After gap analysis between As-Is and To-Be architectures, the action plan of implementing ERP could be developed and followed as the EA transition plan.

Also Infosys (2009) asked 173 respondents about advantages of EA. In accord with this survey, the most important benefits of EA are classified as business and IT alignment, business process improving and standardizing, increase business process flexibility, help in application and IT portfolio management, cost reduction, decrease risk and time of IT projects, improve information flow in organization, help IT innovation, increase customer satisfaction, business process change management, increase value creation of IT, improve quality of IT services, and help organizational change. Furthermore, the main focuses of EA have been integration, Service Oriented Architecture, and security.

On the other hand, Schöenherr (2009) has reviewed 126 publications on EA and categorized the drivers of EA program based on academic articles. He has classified the drivers of EA into two main categories: internal and external. Referring to his research, the most significant internal reasons for EA have been "IT-business alignment, cost reduction, standardization/consolidation, and management/governance". Also main external drivers for EA have been "Clinger-Cohen Act, Sarbanes-Oxley Act, Basel II, and Solvency II". Sarbanes-Oxley Act (SOX, 2002) is a US Federal law which came into force in July 2002, after accounting scandals of Enron, Tyco International, Adelphia, Peregrine Systems, and WorldCom companies which led to widespread financial loss of investors and decreasing public confidence. The Sarbanes-Oxley Act forces public companies to implement corporate governance and internal control assessment in order to ensure that the executive management directs company align with investors benefits. The EA models bring about transparency of stakeholders' concerns, business processes, and responsibilities of people. Thus the EA can help companies comply with Sarbanes-Oxley requirements as a security related regulation.

By reviewing survey of Schekkerman (2005), we can see the trend of security architecture development, shows a considerable growth. He described the reasons of this growth as several rules and regulations such as SOX and Basel II. Also according to the survey Infosys (2009), security is the third focus of EA programs between 18 important focuses of EA.

2.1.3 Challenges of Enterprise Architecture

As Spewak (1994) mentioned in the Enterprise Architecture Planning Methodology, the most important challenge of EA is turning to a bunch of documents that collects dust on a shelf. He also recommended useful course of actions to develop doable EA blueprints and implement results of EA. If organization could not implement outcomes of EA, not only would the spent time and money on EA be useless, but also the considerable profits would be lost because of lag in implementing solutions for business. According to the

published best practices of CIOs in implementing EA (Stenzel, 2007), emerging EA with IT governance increases chance of implementing EA results.

If we consider EA as a planning approach, like other planning processes, long time of developing EA could threat validity of solutions because of rapid changing business requirements, technology trends, and environmental factors such as compliance needs. (Kaisler et al., 2005; Finkelstein, 2006)

Results of EA should be understood, accepted and believed by enterprise stakeholders such as business and IT staffs and management (Kaisler et al., 2005; Chen et al., 2008). If they do not believe EA results they would not be motivated to overcome organizational resistance against suggested changes (McGovern et al., 2003). As trend of EA development shows, transferring EA knowledge to the enterprise and involving internal employees and managers in EA program could be a useful approach in implementing EA results (Finkelstein, 2006).

Developing EA artifacts seems no easy task. EA is complex because it includes different types of proficiency and backgrounds. The experience of enterprise architect is a vital factor in EA; therefore, it seems difficult to teach and apply EA (Wegmann, 2003). Also there are some problems in maturity of EA frameworks, methods and tools which leads to disintegration of EA artifacts. Especially EA frameworks and methods do not effectively support developing To-Be business architectures (Shah et al. 2007).

Since most results of EA are not tangible, it is not easy to justify the investment on EA. Identifying the main stakeholders of EA and assess the satisfaction of these stakeholders could be useful approach to justify EA cost (Infosys, 2009; Kaisler et al., 2005).

The Chief Information Officers (CIO) of organizations are one the most important stakeholders of EA. Lindström et.al (2006) evaluated the harmony between EA frameworks and CIOs' concerns by a survey in which Swedish CIOs prioritized their concerns, and then the result of survey is compared with DoDAF and Zachman frameworks. According to their findings, the main deviation is lack of decision support mechanisms for IT organization in EA frameworks which could be improved by aligning EA with IT governance and IT portfolio management.

As a main result of this section we can conclude that one of the most significant challenges of EA is that EA frameworks and methods are not completely developed yet; therefore, in order to improve EA frameworks, it is important to evaluate different EA frameworks in terms of supporting security concerns of stakeholders.

2.1.4 Enterprise Architecture Concept

There is no accepted universal definition for enterprise architecture (EA) in research communities and industry (Hjort-Madsen 2009, p.22); however, most of the definitions generally agree that “architecture is about the structure of important things (systems or enterprises), their components, and how the components fit and work together to fulfill some purpose” (Shcekkerman, 2004, p.21). There are several studies investigated the different definitions of EA. Langenberg and Wegmann (2004) have reviewed eighty academic publications in which explicitly noted “Enterprise Architecture”. According to their survey, EA is a young but growing discipline which is developed more by IT consulting companies, and there is a lack of basic academic research in EA field.

In addition, Chen et al. (2008) have reviewed the development of enterprise architecture. According to their findings, since 1985 to 2000, researchers worked on architecture for enterprise integration with focus on business requirements rather than technological requirements. They also argued the fact that since 2000, it has been a shift from developing architectures for enterprise integration to interoperability; however, they could not define concept of architecture to develop interoperable systems.

Also, Ahmadi (2010) has reviewed different definitions of EA regarding basic and recognized research groups and communities in EA. According to his research, EA is considered as an approach in enterprise integration, enterprise engineering, business and IT alignment, coherency management, information systems planning, and strategic transformation based on background and conception of researchers in different fields.

Furthermore, Khayami (2011) has analyzed the famous definitions of enterprise architecture and extracted qualitative specifications of enterprise architecture as “alignment, convergence, maintainability, integrity, reliability, efficiency, security, and usability”.

Moreover, Schöenherr (2009) has reviewed the literature of enterprise architecture concept in order to define a common terminology. He has analyzed the trend of research on EA with a quantitative approach. He found out that most of the papers contributed to EA best practices; also, most of the publications have not practical justification and just represent some theoretical concepts or methods.

John Zachman (1987) defines enterprise architecture concept as “set of descriptive representations that are relevant for describing an enterprise such that it can be produced to management’s requirements and maintained over the period of its useful life”.

The ISO 15704 (2000) defines enterprise as “one or more organizations sharing a definite mission, goals and objectives to offer an output such as a product or a service.” Also according to this standard, “an architecture is a description of the basic arrangement and connectivity of parts of a system (either a physical or a conceptual object or entity).”

CIO Council of USA (1999) has defined EA as “a strategic information asset base, which defines the business mission, the information necessary to perform the mission, the technologies necessary to perform the mission, and the transitional processes for implementing new technologies in response to the changing mission needs.”

Wegmann (2003) defines enterprise architecture as a discipline to organize enterprise resources that guide enterprise in its evolution towards its strategic goals.

Chen et.al (2008) explained enterprise architecture concept as a skeleton like in civil engineering which help envisioning future of the system. In this approach, EA is a kind of skeleton which emphasizes on crucial features of system which could be the preliminary phase of design. Also they pointed out that enterprise architecture is a means of talking to stakeholders that enables stakeholders to define their concerns and expectations in the early phase of system designing. In fact, the role of architect is addressing expectations and requirements of stakeholders which should be addressed in later detail designing phase.

IEEE has defined the architecture concept and developed ANSI/IEEE Std 1471-2000 as a standard for architecture which has been referred by most of the later frameworks such as DoDAF and MODAF. According to Hillard (2000) architecture is defined as the “fundamental organization of a system, embodied in its components, their relationships to each other and the environment, and the principles governing its design and evolution”.

2.1.5 Enterprise Architecture Frameworks

As history of EA shows, EA is characterized by EA frameworks. Zachman (1987) defined concept of EA with his framework, and next steps continued by development of EA frameworks. EA framework is a conceptual structure of EA elements and their relationships which describes logical way of thinking to the EA (Inmon et al., 1997). Mykityshyn et al. (2007) defines EA framework “as a plan of how to organize and present enterprise architecture”. There are several EA frameworks which organizations adopted to their operational needs and intended uses (Shah et al., 2007).

According to the review of EA frameworks, it is evident that each EA framework has been developed appropriate with particular context and requirements of a specific group

of enterprises (Shah et al., 2007). But generally, the EA frameworks are driven by the concerns of various stakeholders (Mykityshyn et al., 2007). Chen et al. (2008) describe EA as a means of communication among different stakeholders of enterprise. In fact, stakeholders of EA have concerns which should be reflected in viewpoints and views of EA frameworks (Figure 2.2) (Hillard, 2000).

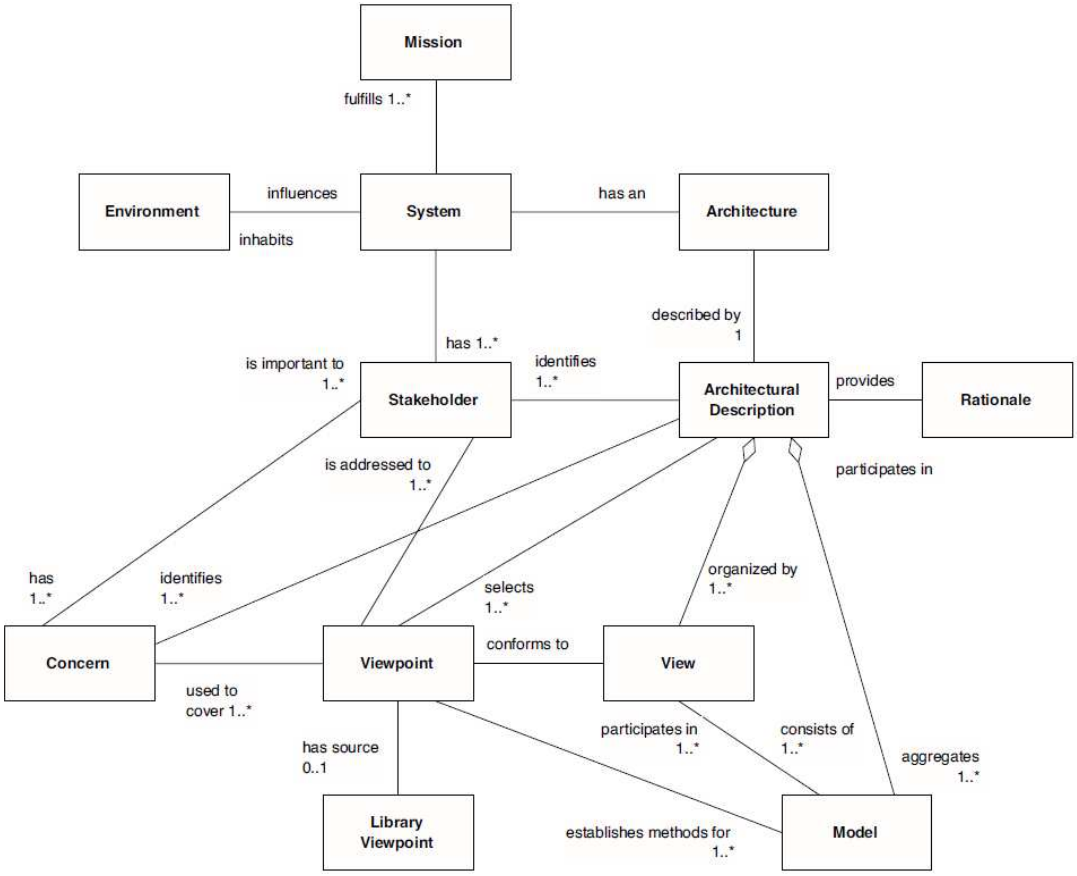

Figure 2.2: Meta-model of architectural description (Hillard, 2000)

Stakeholders of EA are the representatives from business or IT department which affect by EA results (Boh et al., 2007). EA stakeholders have different roles regarding using or building architectural descriptions. The main groups of stakeholders are architects and acquirers/customers (Hillard, 2000). Raadt and et al. (2008) have described the second group of stakeholders (customers) regarding their role and level in enterprise as shown in

Table 2.1. In this table, columns show main components of EA and rows represent organizational level of stakeholders. For example, in the third column from left we have Information Systems (IS), and first row shows the Enterprise level which means CIO is an Enterprise level stakeholder of Information Systems blueprints.

Table 2.1. Key EA Stakeholders, their aspect areas and organizational levels (Raadt et al., 2008)

	Business	Information	Information Systems (IS)	Technical Infrastructure (TI)
Enterprise	• CEO, CFO, COO	• CIO	• CIO	• CTO
Domain	• Head of BD/BU • Business change manager	• DIO • IT change manager	• DIO • IT change manager	• Platform manager • Platform subject matter expert
Project	• Business project manager • Business process designer	• Information analyst	• Software development project manager • Software designer/architect	• Infrastructure project manager • Infrastructure engineer
Operational	• Operational business manager • Business process engineer	• Data administrator	• Application management • Application administrator	• Data center management • Infrastructure administrator

Concerns are the crucial interests of stakeholders in the enterprise which affect enterprise behavior. Concerns are related to the common aspects of organization and functions of enterprise. Concerns include enterprise considerations such as security, corporate governance, risk, cost and benefit, and etc. (Schekkerman, 2004). There are some studies on concerns of each stakeholder. For instance, Lindström et al. (2006) reviewed the concerns of CIO as an important stakeholder of EA. According to their findings, main concerns of CIOs are as follows:

1. Business cost reduction
2. Improve the quality of the interaction between the IT and business
3. Provide new IT solutions to support business
4. Improving quality (security, performance, …) of IT systems
5. Improve the quality of business services or products
6. Improve the quality of procurement, acquisition, and maintenance IT solutions
7. Develop new business services or products for customers
8. Improve the maintainability and modifiability
9. Cost reduction of hardware and software
10. Cost reduction of IT organization
11. Provide new IT solutions for IT organization

As we can see above, security related concerns are ranked as fourth important concerns of CIOs between 11 main concerns. Also security is considered in several studies as one of the growing concerns in enterprises (Kaisler et al., 2005). But security is addressed

differently in EA frameworks, and each EA framework has its particular method to cover security concerns. Unluckily, there is no solid published research on comparing EA frameworks regarding security concerns; however, there are several comparative studies on EA frameworks (Namkyu et al., 2009; Alghamdi et al., 2010; Franke et al., 2009; Leist et al., 2006; Mykityshyn et al., 2007).

As a main result of this part, we can conclude that EA is a means of communication among stakeholders, and EA framework is a logical structure to address main concerns of stakeholders. Since security is a growing concern of stakeholders, EA frameworks has to address security concerns appropriately, but as the EA challenges shows, the EA frameworks do not completely support enterprises achieve goals of implementing EA.

2.2 Security Architecture

In this section, firstly we review the concept of security as the key concept in our research which leads us to today's most important security issue "Information Security". Then we study the history of information security which shows that with new innovations and development, new threats came along. According to our findings, information security concerns are getting wider because of the growing convergence of business and IT. Hence enterprises start experiencing shortcomings in security programs and systems. Where "Traditional Security" tried to address some of these shortcomings based on its military model like Bell LaPaudla, Biba ,Clark-wilson, Brewer and Nash model (Chinese wall model), Graham Denning security model, and security standards, but still essential requirements are seriously missing. Therefore, it becomes ever more important for enterprises to plan and develop a qualified framework which covers information systems security, business continuity planning, and disaster recovery. This framework is a holistic view to security that combine traditional security with the security of IT based enterprises (Brunnstein, 1997; ISC). The summary of findings shows that the current information security landscape is moving toward a strategic approach, which nowadays commonly referred as "Information Security Architecture" (Theoharidou et al. ,2005; Anderson, 2007; Dlamini et al, 2008). This section aims to review concept, history, and goals of Security Architecture (SA). Studying history of SA helps us to find historical dependencies of SA and EA. Also reviewing goals of SA development makes it possible to evaluate different strategies of SA development in terms of effectiveness. Since security is a wide concept it is crucial to determine scope of security in this research; therefore, we start this section by discussing concept and scope of security.

2.2.1 Security Concept

As the human civilizations changed throughout the history, the form of humans' assets, threats, and the way of protecting them has also changed. In the early societies and even till the end of 1980, security was limited to military issues and the security was defined in the ability of military for war and bringing peace after war. (Internet 3)

Bayle (1988) defines security "the act of minimizing the risk of exposure of assets and resources to vulnerabilities and threats of various kinds" (Bayle, 1988). The word security is always tied with two words, control and risk. According to Kim and Leem (2005) risk and control are cause and effects since "Controls are implemented to mitigate risk and to reduce the potential for loss which may be caused by the risk."

But now security is not simple as the past because the whole world is connected through digital communications. Governments, public and private industries, military and educational institutions, and other computing environments become increasingly interconnected through information superhighways (Tudor, 2006) and information continues to play an important part in creating competitive advantage (Porter et al., 1985). Hence security has gradually evolved from addressing military issues to managing informational issues with a huge impact on organizations' economic growth and competitive advantage. In fact, in the information age, information security has become a main concern of enterprises.

2.2.2 History of Information Security

The word information security may subconsciously remind computer or systems, but in fact information security came into existence even before computers. The security of information became important when humans learnt to write and starts to transfer, store and process information. Even later with the invention of telegraph and telephone encryption codes were developed to protect the secrecy and confidentially of transmitted data and information (Russel and Gangemi, 1991).

The late 1940s until the early 1950s that were known as "Down of computing", the first generation of mainframes came into existence. The main security issue of this time was related to physical security of information storage and protecting them from loss or unauthorized access (Dlamini et al, 2008). Information security was not limited to physical security but later in 1960s up to the 1970s, when terminals and networking enabled users to access and use remote connection, a new risk as "Information Transmission" added to the information security field. As a result of the new risk, data could be accessed by unauthorized people or outsiders. Therefore, in late 1970s, the

concept of user identification and authentication came into existence. The next treat was password cracking and password sharing, so that security policies enforcing the use of passwords and avoid outsiders' access came into existence. Gradually, with the existence of terminals and networking, mini computers came in and the number of people with personal computers increased and modems and terminals get cheaper over the time. Parallel with the expansion of computer usage, different access controls and confidentiality models introduced. Later with the entrance of APARNET as the world's first packet switching network a new dimension of information security arose (Denning, 1999). During this time, privacy of information became an issue that caused US government to subscribe the Privacy act of 1974 to protect people personal information recorded in system (Rusell and Gangemi, 1991).

1980s was the introduction of personal computers when everyone starts to have his/her owns computer and companies began to rely on computers for business functions and processes (Rusell and Gangemi, 1991). The usage of computers and IT infrastructure brought a new concept called as "Business Convergence" that gradually became a business threat. Yoffie (1997) and Rold (2002) believe that the business environment is convergence, which means two or more business units are merged together to overcome the limitations of the business. Business convergence is a strategy that merges business, telecommunication and networking, information and technology, content and services models of an enterprise to make a creative business model that results in competitive advantage. At this stage, threats such as computer viruses, worm, and computer fraud and information abuse appeared (Denning, 1991). By moving toward 21st century, enterprises became more dependent on IT infrastructure, and as it becomes easier to exchange information, it becomes harder to protect information. With the digital communication through information highways now, all the government sectors and communities are targets of "Information Warfare". Information Technology makes the data theft and exploitation easier, and attackers have evolved from fans to professional hackers (Gelbstein, 2006). In this era, new threats like financial threats spam and phishing in form of SMS (short message service), mail and MMS (multimedia message service) appeared (SANS, 2007). At the same time, the involvement of online payment systems and web applications in humans' everyday life and the new concept of cloud computing that integrates all the electronic devices like laptops, smart phones, personal digital assistants, increased the possibility of more threats (Dlaimini et al, 2008). Security goes even beyond information theft when some attackers use armed force against opponents (Tudor, 2006). Some attack cases like September 11 brought the message that all the enterprises must be alert to the possibility of new kind of threats and attacks at all times (Dlamini et al, 2008).

With appearing new form of threats security issues became more important. Therefore, security and privacy acts, National Infrastructure Protection Centers (NIPC) like Homeland Security organizations formed and different security management strategies like models, standards and frameworks came into existence (Tudor, 2006; Air Force Doctrine Document, 2006). Indeed many government agencies started to reform in 2003 with a new security effort to protect organizations against unthinkable and extraordinary disasters and attacks (Air Force Doctrine Document, 2006).

2.2.3 Approaches of information security management

According to Caralli (2004) there is no lack of models, standards, guidelines or best practices related to information security. In fact there are more than 80 best practices being used. But in reality, none of them can completely respond to the security concerns. In order to understand the reason of this fact, we have to study the past and current security management strategies. Therefore, in this section we will go through the different foundational tools, techniques and methods that have been used to assure the enterprise security at a certain level. We have classified the major security effort as following:

- Intuitive , critical success factors (CSF) method
- Security models
- Check lists ,standards and best practices (Guidelines)
- Security architecture

The approaches presented above seem to represent the most important security management approaches. The naming and order is derived from Caralli (2004) and Zuccato (2002) papers.

Intuitive, Critical Success Factors (CSF) method

The intuitive approach is mostly used in small businesses where there is no one dedicated to security. In this approach, management treats security if feels necessary. This approach has a very isolated manner to security that makes it tough to qualify the security threats. And normally enterprises never go for this approach. (Zuccato, 2002)

Also CSF (Critical success factors) method for security could be considered as a model to define and prioritize the essential security issues of an enterprise. Therefore, managers could consider the most appropriate approach to solve them. (Caralli, 2004)

Security Models

Different security models have developed, and each model supports one of the core principles of the information security: confidentiality, integrity and availability. Bell-Lapadula is a confidentiality model while Biba and Clark-wilson are integrity models. There are still some models like Brewer and Nash model (Chinese wall model) and Graham Denning model that support availability. (Nash and Brewer, 1989; Clark and Wilson, 1987; Bell, 2005 and Biba 1977)

Check lists, standards & best practices of information security

In compare with intuitive approach, checklists are a good step to move from an improper and unskilled approach toward a structure that assures security up to a certain level. BS7799-1 and Basic Protection Manual (BSI, 2002) are the most well-known checklists (Zuccato, 2002).

Apart from checklists, security standards are a list of artifacts and techniques that cover all three aspects of the security (Confidentiality, Integrity, Availability) (Yang et al., 2010) and is used to secure different area of enterprise. Some of them focus on managing information security like ISMS and BS7799 (ISO27001), while some standards like COBIT and GMITS (Guidelines for Management of Information Technology Security) help managers to manage the risk associated with IT and planning, management and implementation of IT. Some other standards like ISF (Information Security Forum), GASSP (Generally accepted system security principles) and BSI IT (baseline protection manual) are used as a general guideline and good practice for information security. Even some standards like ISO/IEC consist of different sub-standards and cover many different areas such as security policy and organization (Ekstedt and Sommestad, 2009).

Another form of security management is best practices derived from software industry. This approach is based on a software development practice and it is more than just a checklist and includes comprehensive methodology to impelement (Zuccato, 2002). The most important disadvantage of best practices and standards is that each best practice just covers one dimension of enterprise security such as network and physical security.

2.2.4 Security Architecture Concept

In the previous section, we reviewed the most common approaches of security management, and we found out that none of them fully supports the enterprise against threats. In fact, we need a holistic approach to plan security. One of the main reasons of approaching to holistic view is that today information technology works as a driver for

businesses to achieve their goals while in the past there was only a business-driven approach to security. The new approach creates a complex and disjoint security infrastructure which is hard to manage and uneasy to see the gaps. For instance, the security concerns of CEO, CFO, COO, CIO and CTO are different; therefore, it is difficult to achieve an end-to-end security approach that supports business goals, operational requirements and protect against internal and external attacks. To ensure that all security domains work together in alignment with business strategy, enterprises need for a holistic view otherwise the enterprise's vulnerability would increase because of IT and business strategy misalignment. (IBM, 2008)

The lack of interoperability, business convergence, and business partnership are some other important drivers that encourage enterprises for a holistic approach to the security (Keem & Leem, 2005). On the other hand, after widespread use of enterprise architecture, as a holistic approach to manage main concerns of enterprises, the "Information Security Architecture" concept came to existence (Michelle et al., 2009). However, the holistic view to security was considered before EA and "security architecture" as a modeling view of the security has been used by security technicians to define security architecture of database or network before appearing EA. But current concept of information security architecture is defined based on EA approach.

According to our study, there is no "one fits all" definition of enterprise security architecture but rather it consists of different security guidelines that come in forms of services, models and standards, each of these must work well individually and in relation with other elements to achieve the overall enterprise security.

Tahajod et al, (2009) defines security architecture as following:

… *"Traditionally, security architecture is a document, which specifies which security services are provided how and where, in a layered model. Originally the model typically referred to OSI layers and specified the security elements or services and the mechanisms used to provide them"*

The main purpose of security architecture is integration between different security elements (network, information, etc.) and providing a single document (Tahajod et al, 2009) that specifies the security services. Sherwood (2005) in his book "Enterprise Security Architecture: A Business-Driven Approach" discussed that Security architecture is trying to bring a new vision of enterprise security by saying that

…security is too important to be left in hands of just one department or employee; it's a concern of an entire enterprise. Enterprise Security Architecture shows that having a

comprehensive plan requires more than the purchase of security software -- it requires a framework for developing and maintaining a system that is proactive.

It is important to acknowledge that there is no single definition for a security architecture that works across the thousands enterprises and organizations in existence today since each enterprise has its own culture. For example, the security architecture that is appropriate for a bank will not work for a hospital, university or military sector. Therefore, enterprise security architecture must respond to the context and culture of an enterprise. (Peterson, 2006; Luker & Petersen, 2003)

Prentice Kinser (2007) defined the security architecture as "a cohesive security design, which addresses the requirements (e.g. authentication, authorization, etc.) and in particular the risks of a particular environment/scenario, and specifies what security controls are to be applied where".

Open security architecture (OSA) defines the security architecture as "The design artifacts that describe how the security controls (= security countermeasures) are positioned, and how they relate to the overall IT Architecture. These controls serve the purpose to maintain the system's quality attributes, among them confidentiality, integrity, availability, accountability and assurance." (Internet 4)

Tom Scholtz (2008) defined information security as "the process that delivers planning, design and implementation documentation (artifacts) in support of the program. The architecture framework is a consistent reference model for structuring the process and the deliverable documentation."

Tom Scholtz, in another paper with F. Christian Byrnes and Jay Heiser (2005), said "The architecture provides the principles, methods (for example, domain structuring, trust modeling) and templates (such as security infrastructure architectures, application security templates) for selecting, designing and implementing appropriate security solutions."

According to Swiss Information Security Society (SISS), "security architecture is a cohesive security design, which addresses the requirements (e.g. authentication, authorization, etc.) – And in particular the risks of a particular environment/scenario, and specifies what security controls are to be applied where. The design process should be reproducible." (Thorn et al, 2008)

Also Peterson (2006) defines "security architecture as a unifying framework and reusable services that implement policy, standards, and risk management decisions. The security

architecture is a strategic framework that allows the development and operations staff to align efforts, in addition the security architecture can drive platform improvements which are not possible to make at a project level."

By reviewing different definitions, we can find some common keywords like "Description (policy, procedure, model, artifact, and document)", "Requirements", "Controls", "and "Risk".

Also as a summarized concept from different definitions information security architecture is a practical framework that:

- Act as a reference for security assessment
- Act as a reference for planning and implementing security
- Integrate the security processes within and between different layers of an enterprise
- Standardize the process of information security
- Helps to use the shortest and most concrete way to process a security issues
- Provide a standard procedure that can be evaluated

Also there are certain reasons why enterprises use security architecture rather than other security management approaches. After reviewing different publications we found the followings as main reasons:

Some believe that enterprises use security architecture because it reduces the cost of security and helps for change management (Office of CIO of Ministry of Citizen's services in British Columbia, 2010) while some others discussed that the reason for using security architecture is that it helps for a better integration between security elements, security services and security mechanism and at the same time it allows the business and security staffs to align their efforts (Peterson, 2006; SABSA, 2008). There are still some others arguing that security architecture works as a holistic view that specifies which security services are provided, how and where (Office of CIO of Ministry of Citizen's services in British Columbia, 2010;Kim & Leem, 2005; Ekstedt and T. Sommestad 2009; Killmeyer, 2006; Lowman and Mosier, 1997; Shiozaki et al, 2006; Sachitano et al, 2004). And lastly compliance is another reason that makes enterprises to apply SA (Preez and Pieterse, 2009). Therefore, main SA goals could be concluded as holistic approach, security & business alignment, Integration, change management, security requirements analysis, security cost reduction, and compliance.

2.2.5 History of Security Architecture

Tracking the history of SA shows that the concept of security architecture has been mainly introduced and discussed since 1995. Where some researchers like Henning (1996), DeLooze (2001), Zachman (2001) and Heaney et al (2003) introduced an integrated approach or a holistic view to reduce the complexity of enterprise information security using Zachman framework.

On the other hand, since 1996, some other researchers started to discuss security architecture as a standalone framework. SALSA is an example of early security architecture frameworks that has been developed in 1996 by john Sherwood. SALSA is a five layer model that defines a process for enterprises to decide for their security. Its primary objective is that everything is based on analysis and understanding business requirements for security. In the first layer (business requirements) SALSA tries to address the business requirements for security. In second layer (security strategies) it addresses the strategies to meet the business requirements. The third layer (security services) will define the security services of the selected strategy in layer two. In fourth layer (security mechanism) the mechanism of implementing each security service is discussed. And the last layer (security products and technology) maps the mechanism with the available technologies (Sherwood, J. 1996).

In 1997, US Department of Defense developed DGSA as a goal model for security architecture as part of TAFIM. DGSA works as a guide for developing specific security architectures by defining security services and security mechanisms. (Lowman & Mosier, 1997)

In 1998, Open Architecture Security for Information Systems (OASIS) has been developed with the purpose of integrating the isolated security systems within enterprise (Essmayr & Kapsammer, 1998). Later in 2004, Sherwood introduced a new security architecture called SABSA that stands for Sherwood Applied Business Security Architecture. SABSA was a framework that has the same structure as Zachman Framework (SABSA, 2008). Also recently, some newer security architecture frameworks like VIsualizing Enterprise Wide Security (VIEWS), Gartner Enterprise Information Security Architecture (EISA), RISE, AGM and intelligent Service oriented EISA came into existence. (Brennan et al., 2004; Wikipedia, 2010; Anderson & Rachamadugu, 2008; Shariati et al, 2011)

2.3 EA & SA relationship

By comparing EA and SA histories we can easily find out that SA has been created as a part of EA (Michelle et al., 2009). In fact, holistic view and modeling approach as main principles of enterprise architecture are addressed in SA. However, need for a holistic perspective on security mentioned before introducing EA, and architectural models were used before by security technicians to represent security of database or network. But the question is that why EA has not included SA like other sub-architectures such as business, application, data, and technology architectures. In other words, why are we studying relationships between EA and SA while SA should be a subset of EA? What are the differences between SA and other architectures? Answer to this question would help us analyze different strategies of SA development regarding EA.

First, EA, as a means of facilitating communication among stakeholders, seeks to standardize language of describing different elements of enterprise such as business process, application, data, and technology. The technical nature of these elements helps different enterprises to define their process, application, data, and technology in a standard way. But information security is not just a technical concept; in fact, the several none-technical factors such as political, cultural, and social issues are affecting security (Blatchford, 1996). Therefore, it is not easily possible to standardize definition of these none-technical factors affecting information security. That is the reason information security architecture could not be defined universally but it should be defined appropriate with the context of each organization (Peterson, 2006; Luker & Petersen, 2003).

Second, as Wegmann (2004) pointed out in his research, EA is a concept developed by consulting companies; thus EA has mainly evolved by consulting companies based on need and request of customers. In other words, request of organizations for business, data, application and technology architectures have led to developing these concepts under the umbrella of EA. By reviewing the history of information security, we can see different models and approaches to manage security were grown based on developing IT and increasing access to the information. Hence, need for information security comes after developing information systems and sharing information. That is the reason information security architecture approach introduced about 10 years after EA. Also, in enterprises, need for a proactive plan of security could be seen after developing IT.

2.4 SA & EA Frameworks

In order to answer third research question about supporting SA by EA frameworks, we have reviewed security concerns in Zachman, DoDAF, TOGAF, FEAF, and DNDAF as

the most famous open EA frameworks that have mostly been studied in academic researches.

2.4.1 Security and Zachman Enterprise Architecture Framework

Zachman EA Framework is a conceptual matrix to classify architectural models and descriptions. Rows of the matrix represent different perspectives in describing an information system (Figure 2.3):

1- Planner describes scope of IS.
2- Owner explain enterprise model.
3- Designer represents a logical model of system.
4- Builder redraws a technology model.
5- Subcontractor who specifies detail of their parts in component model.

The columns of framework represent main abstractions in describing IS in response to the six English interrogatives: Entities (What?), Functions (How?), Locations (Where?), People (Who?), Times (When?), and Motivations (Why?). Each cell describes a specific focus of IS from particular perspective. Collection of models and descriptions representing all cells of a row, describes IS from that perspective; also, all of the models of a column explain that abstraction of IS. (Sowa & Zachman, 1992)

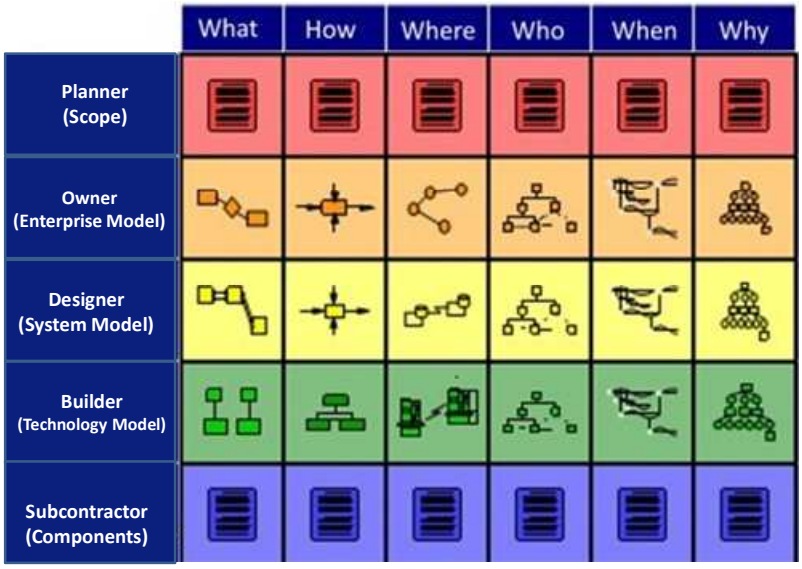

Figure 2.3. Abstractions and perspectives of Zachman EA Framework (Sowa & Zachman, 1992)

The Zachman framework is a conceptual framework which defines the viewpoints and abstractions of enterprise architecture. In fact, Zachman has not suggested any methodology, notation, case tools, and reference model to develop EA. Therefore, he has not considered explicitly security concerns, but some security architecture frameworks have been developed based on Zachman Framework. The most important Zachman-based security architecture frameworks are Heaney (Heaney et al., 2003), DeLooze (2001), and Henning (1996) Frameworks. These SA frameworks have considered security as an enterprise and tried to apply perspectives and focuses of Zachman framework into security concept.

The Heaney et al. (2003) added a column to the Zachman framework to "integrate Information Assurance (IA) into the all levels of enterprise engineering". According to their approach, adding IA as a separated column to the Zachman framework help IT men address IA in the early phase of system design and development. They also pointed out the fact that current EA frameworks do not address IA explicitly, thus IA cannot be analyzed separately and integrated with other architectures. In fact, Heaney tried to integrate the IA by adding a column to Zachman Framework, but it seems his approach just succeed to address security concerns explicitly, and could not be used to integrate IA into other architectures because the security cannot be separated from other abstractions such as data, process, people, and location.

Delooze (2001) tried to use Zachman Framework in order to apply security to the enterprise. In accord with his approach, the organizational security policy could be implemented in the planner perspective of Zachman Framework. Moreover, according to the security policy, data groups of enterprise (customer data, employee data, and etc.) should be defined regarding importance to the business. At the next step, it should be determined who could access each data group and where these people are located. For example, based on these definitions, the http router rules can be set, and firewall of application layer can control information exchanges between applications. The Delooze approach in using Zachman framework to address security is a holistic view and could be integrated with other EA models appropriately. For instance, the CRUD matrix, as an EA artifact which shows the information manipulating of business functions, can be used to determine data access control.

2.4.2 Security in Federal Enterprise Architecture Framework (FEAF)

The FEAF (CIO Council, 1999) is a mechanism to manage development and maintenance of EA descriptions which describe a structure for organizing Federal resources. The FEAF framework is recommended to use in government-wide efforts, multi-Federal Agency efforts, and when the business and investment scope of activities

include international, state, or local authorities. The FEAF provides some reference models to help Federal Agencies coordinate common business processes, information sharing, systems, and IT investment through Federal agencies efficiently and effectively. The FEAF includes eight main components explored in four level of granularity:

1- **Architecture drivers:** external factors that cause Federal EA to change including business and technological drivers.

2- **Strategic direction:** the guideline of EA evolution to ensure that changes are consistent with Federal direction.

3- **Current Architecture:** business and IT architectural model to represent current state of enterprise.

4- **Target Architecture:** business and IT architectural model to represent future desired state of enterprise.

5- **Transitional Process:** the process to conduct change from current to the desired state in compliance with standards such as migration planning and budgeting.

6- **Architectural Segments:** the main common business and system functions such as “grants or common financial systems” which cross-cut all enterprises.

7- **Architectural Models:** the business and technical models to represent enterprise segments.

8- **Standards:** includes the mandatory and optional standards of data, application, technology, and security which could be used in transition from current to target architecture.

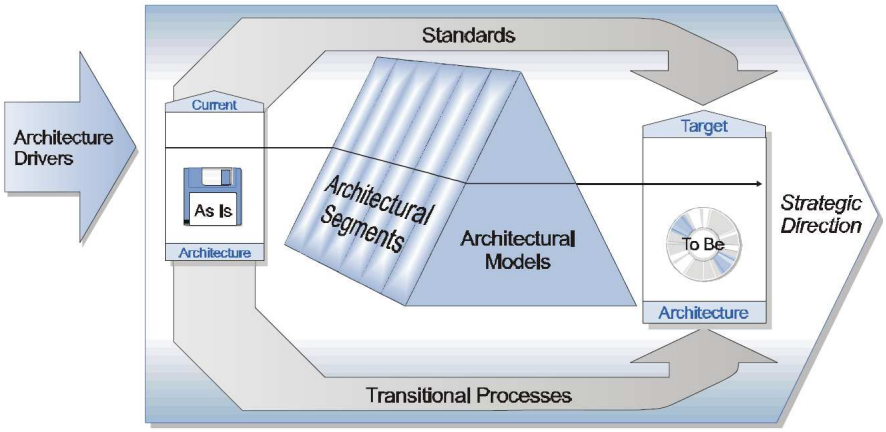

Figure 2.4. FEAF components in Level I (CIO Council, 1999)

Security and privacy have been two main principles of developing FEAF by CIO Council. According to the security principle agencies have to “secure Federal information from unauthorized access”. Also they have to observe privacy right of people to comply with 1974 Act. In accord with this act, public should be given right to provide or not provide information which can be used for other purposes.

In fact, there is no independent security component in the FEAF; however, security standards are included in standard component of the FEAF. Also, according to the Practical Guide of FEA (CIO Council, 2001) information security management is defined as a complementary process which enables enterprise to manage IT effectively.

The most considerable security related attempt of FEAF, is the "Federal Enterprise Architecture Security and Privacy Profile (SPP)" which is developed by NIST & OMB (2009). The security and privacy profile is a "conceptual methodology for addressing information security and privacy requirements". SPP supports different phases of security architecture such as identifying security requirements, requirement analysis and select security solutions. Also, SPP as a reference profile helps agencies understand and integrate Federal information security standards with EA, so that SPP could be considered as a security reference model for FEAF.

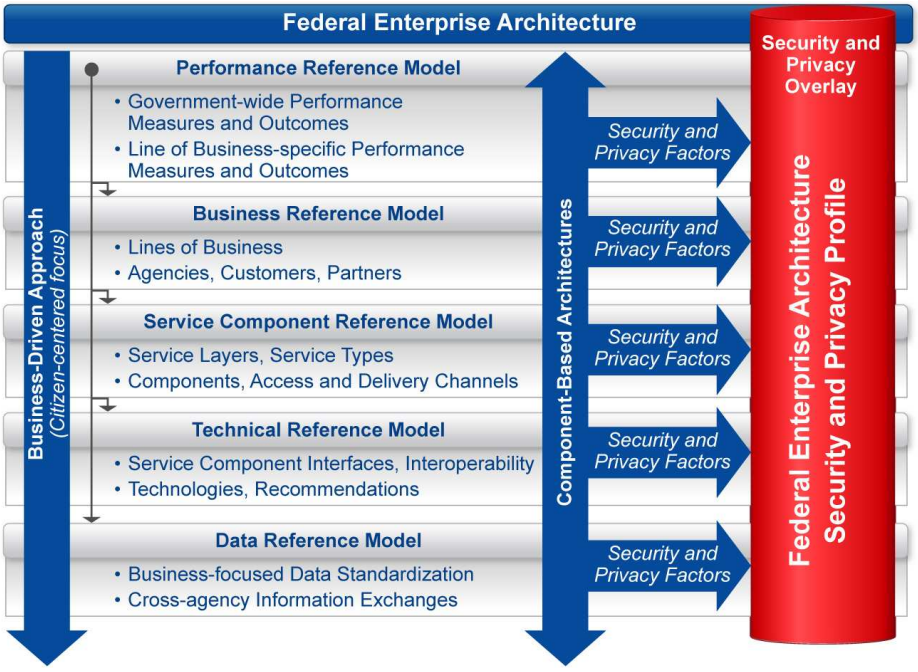

Figure 2.5. FEA Reference Models and SPP (NIST & OMB, 2009)

FEA reference models help Federal agencies to develop their EA models and increase interoperability through standardization. The FEA reference models includes: 1- Performance Reference Model which defines common indicators for performance measurement, 2- Business Reference Model which describes a hierarchy of common business lines, 3- Service Component Reference Model which represent common services supporting common business lines of FEA to reuse common services and decrease costs, 4- Technology Reference Model which determine necessary technical

standards to increase interoperability between agencies, and 5- Data Reference Model to define common data entities and relationships to enhance level of data integrity and information sharing. Adding SPP to other reference models (Figure 2.5) led to layering security over other reference models, and consolidation of security capabilities thanks to the standardization of security architecture. In addition, there is a software assessment tool to support different phases of SPP. For example, this software could help agencies estimate cost of implementing security controls.

2.4.3 Department of Defense Architecture Framework (DoDAF)

Department of Defense of US (2010) developed DoDAF as a mean of representing EA. DoDAF helps stakeholders focus on their specific concerns while they retain oversight of the big picture of enterprise. The focus of DoDAF Version 2.0 is understandable representation of complex EA descriptions and models to facilitate decision-making. In DoDAF, architectural descriptions divided into eight main viewpoints (Figure 2.6) and each viewpoint is described by architectural descriptions, models, and graphical and tabular data. The viewpoints of DoDAF are as follows:

1. ***The All Viewpoint*** *describes the overarching aspects of architecture context that relate to all viewpoints.*

2. ***The Capability Viewpoint*** *articulates the capability requirements, the delivery timing, and the deployed capability.*

3. ***The Data and Information Viewpoint*** *articulates the data relationships and alignment structures in the architecture content for the capability and operational requirements, system engineering processes, and systems and services.*

4. ***The Operational Viewpoint*** *includes the operational scenarios, activities, and requirements that support capabilities.*

5. ***The Project Viewpoint*** *describes the relationships between operational and capability requirements and the various projects being implemented. The Project Viewpoint also details dependencies among capability and operational requirements, system engineering processes, systems design, and services design within the Defense Acquisition System process.*

6. ***The Services Viewpoint*** *is the design for solutions articulating the Performers, Activities, Services, and their Exchanges, providing for or supporting operational and capability functions.*

7. ***The Standards Viewpoint*** *articulates the applicable operational, business, technical, and industry policies, standards, guidance, constraints, and forecasts that apply to capability and operational requirements, system engineering processes, and systems and services.*

8. ***The Systems Viewpoint****, for Legacy support, is the design for solutions articulating the systems, their composition, interconnectivity, and context providing for or supporting operational and capability functions.*

   (DoDAF , 2010)

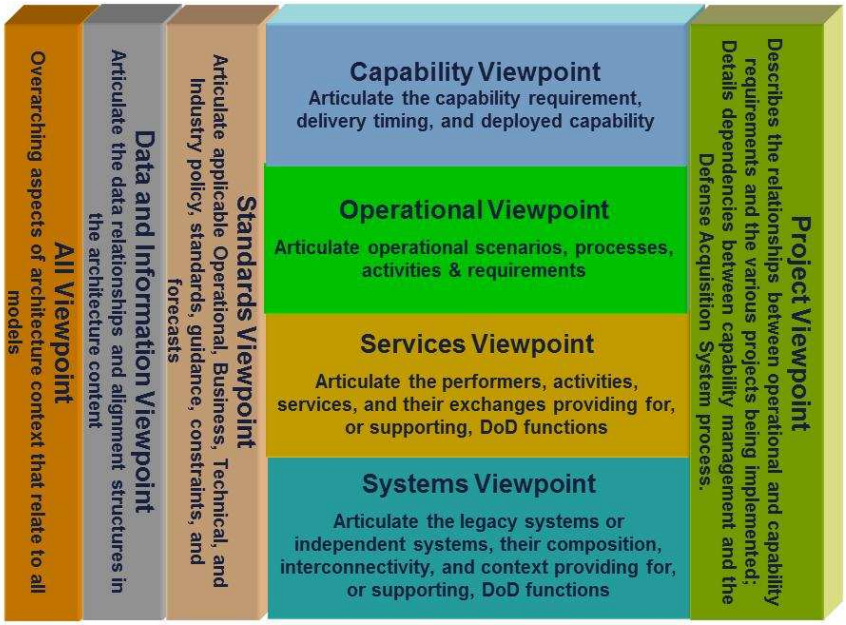

Figure 2.6. Department of Defense Architecture Framework (DoDAF, 2010)

The DoDAF framework has not any specific viewpoint for security. According to the DoDAF (2010), architectural descriptions at any level need to ensure that appropriate security concerns are addressed clearly. The security related data in DoDAF are supports physical, procedural, communications security (COMSEC), Transient Electromagnetic Pulse Emanation Standard (TEMPEST), and Information Security (INFOSEC) concerns. However, there are some critiques on security architecture in DoDAF. For example, Conkling et al. (2009) pointed out the fact that security is considered as an afterthought in DoDAF.

The DoDAF meta-model includes security concepts and attributes which could be used to address security characteristics in EA models. The strategy of DoDAF for addressing security concern is defining required measures to protect capabilities. This strategy

includes risk assessment of capabilities. That is the value and criticality of assets and potential threats should be assessed to define minimum protective measures. In fact, security requirements and related measures could be defined in different viewpoints. For instance, the minimum needed clearance of users could be defined according to the importance of a location, facility, organization or activity. Also, the security concerns of information exchanges between operational nodes could be defined as an attribute of information exchange matrix (OV-3), and the system architect can design system features appropriately to support security requirements of exchanging information. Moreover, security requirements as none-functional requirements of system are considered in Systems Measures Metrics (SV-7). In addition, security standards could be defined in the Standards Profile (StdV-1) of DoDAF. In general, DoDAF has defined the security classification concept as a collection of attributes of each EA product. The security classification is defined as "the level assigned to national security information and material that denotes the degree of damage that its unauthorized disclosure would cause." (DoDAF, 2010).

2.4.4 Security in TOGAF

Open Group Architecture Forum (TOGAF, 2009) developed TOGAF as a collection of models, guidelines, methods, techniques, and tools to develop, implement, and maintain EA. Architecture Development Method (ADM), as the core of TOGAF, explains practical guidelines and methods of developing EA for an enterprise. Also, TOGAF contains and Architecture Capability Framework which describes roles, responsibilities, processes, and organization of developing and maintaining EA in an enterprise. Moreover, TOGAF supports EA development by a complete meta-model of EA artifacts and EA reference models.

TOGAF has addressed security architecture explicitly in the ADM; however, according to TOGAF, it is not a methodology to develop security architecture. The chapter of Security Architecture and AMD is a guideline for architects to avoid missing security concerns in different parts of EA. According to TOGAF, security architecture has its own methods and frameworks and introduces its own non-normal scenarios. That is the IT architect define normative information flow and using IT services, but security architects define the situation that IT service might fails. TOGAF also emphasizes on interacting security architects with other architects in the early phase of EA. AMD has explained the input and outputs of EA and SA in each phase of EA development.

Therefore, like DoDAF, TOGAF has considered security as a background of other EA products such as information exchange matrix and data security diagram as a part of data architecture that shows each actor can access which data.

In February 2011, Open Group (2011) published the Open Information Security Management Maturity Model (ISM3) which helps organizations ensure that security management processes are implemented appropriately and aligned with business requirements. ISM3 includes operational metrics to evaluate maturity of security management processes. The main goal and application of ISM3 in organizations could be controlling the information security management. To put it simply, enterprises can use ISM3 metrics to evaluate their current information security management. At the next step, they can define organization targets for each process and control process improvement annually. So that ISM3 can be categorize as a reference model for information security management.

2.4.5 Security in DNDAF

Department of National Defence and the Canadian Forces Architecture Framework (DNDAF) is a DoDAF-driven EA framework that created to develop EA models and support EA management and EA clients. According to DNDAF there are three main classes of architecture: 1- Reference Architecture as an accepted architecture of a domain, 2- Baseline Architecture as descriptions of current state, and 3- Target Architectures as the models and descriptions of desired state. Also DNDAF defined 14 principles that determine direction of architecture. One of the principles of DNDAF is "Security, Confidentiality, Privacy and Protection of Information". This principal pointed out security as an integral part of design should be considered from initial phase of system design. (DND/CF, 2010, Vol.1)

DNDAF includes eight main views similar to DoDAF, but a new view as Security View has been added to increase visibility of security attributes of other products. The Security View of DNDAF contains three products as below:

1- ***Risk Assessment Document (SecV-1)****: the association of threats, risks and the resulting security control objectives.*

2- ***Data Element Security Matrix (SecV-2):*** *Listing of all data elements used by the architecture along with its security parameters. Included in these parameters are a means of documenting the aggregated security implications for each data element.*

3- ***Aggregated Information Security Matrix (SecV-3):*** *A list of all system data exchanges used by the architecture that may cause potential information aggregation security violations.*

(DND/CF, 2010, Vol.2)

2.4.6 Security in other EA frameworks

Also some other DoDAF-driven frameworks such as Ministry of Defence Architecture Framework (MODAF) have considered security architecture implicitly similar to DoDAF. In addition, Extended Enterprise Architecture Framework (E2AF) has defined an explicit viewpoint for security which is a supportive viewpoint for other architectures. An enterprise architect has to balance security against usability all the time (Schekkerman, 2006).

2.5 Research Model

In order to answer research questions, we need a theoretical framework supporting our analysis. The theoretical framework defines fundamentals of SA development strategies, evaluation of SA development strategies, and SA situation in EA framework. Also it will be used to design our interview questions which help us connect research questions to the interview questions and analyze speeches of interviewees to extract answers of research questions. A brief description of our theoretical framework is represented in Table 2.2. We will explain each part of theoretical framework in following sections.

Table 2.2. A brief description of theoretical framework

Fundamental	**Description**
SA development Strategies	• A totally generic (independent) model of SA development is universally applicable (Sherwood, 1996). • Frequently, security aspects of a system are analyzed and designed separately from other architectures (Heaney, 2002). • Using Zachman Framework to develop security architecture is extremely useful (Delooze, 2001). • To develop enterprise security architecture framework Kim & Leem (2005) have used EA frameworks. • Zachman Framework can be used as a tool in developing security policy of enterprise (Henning, 1996) • EA can be used as a coordination tool to design solutions to the security problems (Pulkkinen et al, 2007) • SA can be integrated into process & infrastructure management by leveraging EA approach (Anderson & Rachamadugu, 2008) • EA can support control management system such as security by providing a better holistic view of IT & business (Ekstedt & Sommestad, 2009) • SA can be developed as a subset of EA (Michelle et al., 2009)
Evaluation of SA development Strategies	• Effectiveness (Holistic approach, Security & business alignment, Integration, Change management, Security requirements analysis, Security cost reduction, Compliance) • Efficiency of SA development (cost & time) • Impact of SA (practicality of outputs) • Performance (ROI, value creation for business, cost reduction)
Situating SA in EA frameworks	• GERA: Reference architecture of EA • EEM: Methodology of EA • EMLs: Modeling language of EA artifacts • PEMs: Reference models of EA • EETs: Case tools to develop EA models and descriptions

2.5.1 SA development strategies

We have reviewed a lot of academic publications on SA and tried to extract and classify different strategies of SA development regarding EA in order to answer Q1 of research. According to our literature review, we reached to a categorization in which there are two main approaches toward security architecture development in relation with EA, a summary of each approach is explained as follows:

1- **Security architecture as an independent approach from EA**: in this approach security architecture is described based on industry accepted frameworks and methodologies as a collection of policies, procedures, processes, structures, and rules to manage security (Tudor, 2006; Shiozaki et al., 2006; Sherwood, 1996).
2- **Security architecture as a dependent approach to EA:** some of studies define security related to the EA. The relationship between security architecture and EA could be classified in three main categories:

   a. **EA as a method could be used to define security architecture**: Since SA is derived from EA, some researchers and professionals have applied EA methods and frameworks to develop security architecture. For example, DeLooze (2001) and Henning (1996) used this approach to plan for security frameworks based on Zachman framework.
   b. **EA artifacts for developing security architecture**: EA artifacts give a complete and integrated picture of enterprise, that is the reason some of security professionals have tried to use EA artifacts to design security architecture. For instance, Ekstedt et al (2009) have investigated the usage of EA blueprints in cyber security analysis.
   c. **Security architecture as a part of EA**: in this approach security architecture has been considered as a subset of enterprise architecture either as a view, reference model, part of methodology, or product. Some common EA frameworks that cover security as a subset are FEAF, DNDAF, E2AF and DoDAF, Heaney et al. (2003).

demonstrates that a number of different approaches are used in the pairing of “SA” and “EA” among researchers.

Table 2.3. Different approaches toward the EA and SA relationship

Reference	Approaches toward building security architecture			
	Independent from EA	Dependent to EA		
		EA as method in SA	EA for SA Development	SA as a part of EA
(Tudor, 2006)	✓			
(Shiozaki et al, 2006)	✓			
(Olivier, 2001)	✓			
SALSA (Sherwood, 1996)	✓			
(Hayashi, 2006)		✓		
(DeLooze, 2001)		✓		
SABSA (Sherwood et al, 2005)		✓		
(Ertaul & Sudarsanam, 2005)		✓		
(Zachman, 2001)		✓		
(Henning, 1996)		✓		
(Tom Scholtz , 2006) Gartner –EISA		✓		
(Pulkkinen et al, 2007)		✓		
(Kim & Leem, 2005)		✓		
(Hensel & Lemke-Rust, 2010)		✓		
(Innerhofer et al, 2006)		✓		
RISE (Anderson & Rachamadugu, 2008)			✓	
(Ekstedt & Sommestad, 2009)			✓	
TOGAF (2009)			✓	
Zachman (Heany et al, 2002)				✓
DoDAF (2010)				✓
DNDAF (2010)				✓
FEAF				✓
E2AF				✓

2.5.2 Evaluation of SA development strategies

In order to answer Q2 about evaluating different strategies of SA development, we need a framework to define measurements of the evaluation. Since there is no theory to evaluate SA development strategies we select an evaluation framework (King, 1988) which has been developed and used in evaluation of Information Systems (IS) planning field. In fact, due to the lack of theory in the security architecture and security planning field, some of the previous researchers such as Young (2010) have applied IS theories to the security planning research area.

According to King (1988), a generic process of IS planning contains IS planning system, outputs which help business performance, informational inputs, resource inputs, predefined goals, and the external standards which affect IS planning. King (1988) defines the IS planning evaluation framework based on relationships between main parts of generic process of IS planning. We have applied the same logic to the SA development as a similar process to IS planning. Since we want to evaluate strategies of SA development, we need just measurements which are meaningful to compare different strategies of SA development; therefore, we have selected three main measurements as shown in Figure 2.7.

1- **Effectiveness of SA development**: how well SA development has met its goals: Holistic approach, Security & business alignment, Integration, Change management, Security requirements analysis, and Security cost reduction (According to literature review results in section 2.2.4)

2- **Efficiency of SA development**: measuring cost and time of SA development

3- **Impact of SA development**: evaluating real and practical impacts of SA on information security of enterprise

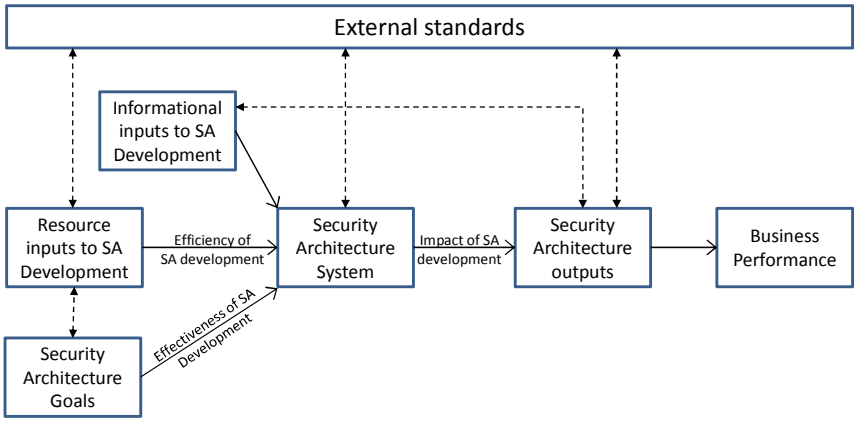

Figure 2.7. Customized IS planning evaluation framework (King, 1988) for SA development

2.5.3 Situating SA in EA Framework

If we want to answer Q3 we have to classify and analyze different parts of EA frameworks regarding security; therefore, we have selected Generalized Enterprise Reference Architecture and Methodology (GERAM) (ISO/IEC, 2005). GERAM is a meta-model of EA and developed by generalizing other EA frameworks. Thus GERAM can be used to evaluate other EA frameworks or components of an EA framework (Noran and Bernus, 2009). Since SA is a subset of EA, we have used GERAM to situate SA in the EA structure. In previous studies, several famous EA frameworks such as DoDAF, Zachman, and TOGAF have been assessed against GERAM (Bernus et al, 2003). The GERAM meta-model to describe EA component and their relationships is represented in Figure 2.8. We have situated SA in EA frameworks regarding EA reference framework (GERA), methodology of EA development (EEM), modeling language of EA artifacts (EMLs), reusable reference models of EA (PEMs), and case tools of EA development (EETs) as the main components of EA. Other components of GERAM describe developed EA artifacts in a particular enterprise.

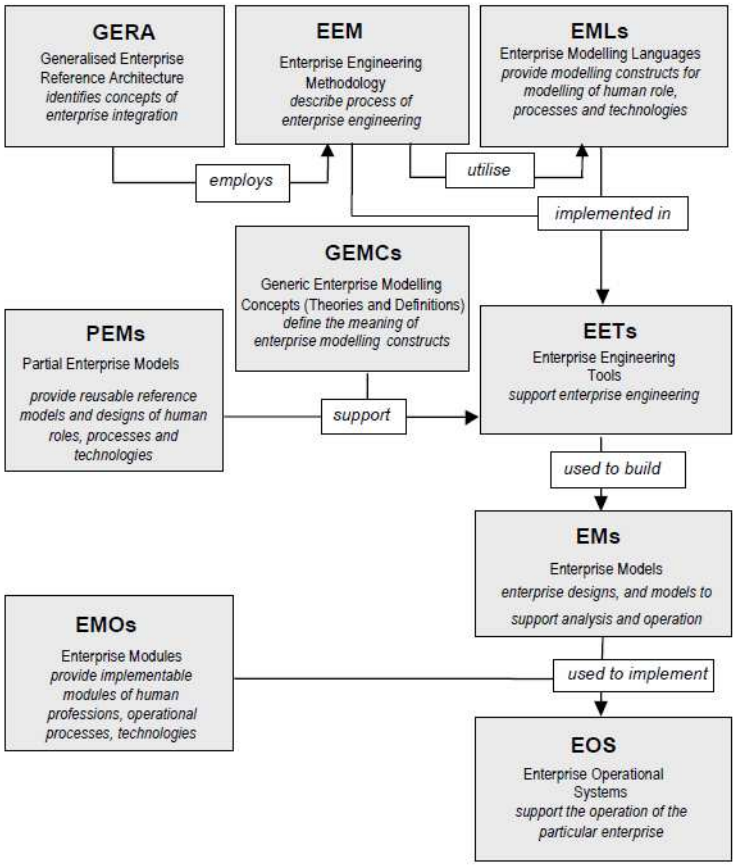

Figure 2.8. Components of GERAM Framework (ISO/IEC, 2005)

3 Research Method

The research method is one of the most important sections in any study because it provides the reader with a clear and precise description of how the research is conducted, what procedures have been gone through and the rational for why such procedures have been chosen (Kallet, 2004). Therefore, a reflexive research method increases the quality and verifiability of our study by paving a clear roadmap and guidance for those who wants judge the results and conclusions of our research and apply our research finding to the further cases.

It is important to acknowledge that the chapter of research method was historically called as “materials and method” to emphasis on the importance of two different aspects that need to be addressed in a research. Materials refer to what we examined and method refers to how we did that. (Kallet, 2004)

3.1 Research Strategies

Prior to our study, we have reviewed different research methods where we selected Template Analysis, Literature review, Case Study, Survey, and Qualitative Interview with experts as candidates for research strategy. Following, we will discuss the rationales for each alternative separately, and we discuss which one is more appropriate for our research question.

One way of answering to our research question could be conducting a template analysis. “Template analysis is the process of organizing and analyzing textual data according to themes” (University of Sheffield, 2011). This approach would help us to understand how different scholars, professionals, and expert communities define the role of EA in developing SA. In this approach, the researchers go through different publications and summarize the result of analysis in analytical tables. King believes that template analysis is a way for analyzing qualitative data (King, 1998). The result of template analysis serves as a basis for other researchers to find where the EA and SA relationship is going. In this research, we followed the same approach where we found the publications from literature review and summarized the result of analysis in Table 2.3 and Table 4.4.

The main reason for selecting template analysis is that the fields of EA and SA are too broad and there are mass amounts of academic and technical publications in these areas. So that obviously we could not read all the publications to find the relationship between these two fields. Therefore, to manage hundreds of articles it was necessary to use

template analysis to compare the viewpoints of different researchers about the relationship between EA and SA.

To evaluate different strategies of security architecture development we could also conduct interview with EA experts who have the practical knowledge of developing EA and SA in different contexts. By choosing this strategy, we would be able to use both academic approach based on literature review and at the same time we gain knowledge from those who are dealing with real life cases.

Thus far we have selected template analysis, literature review and interview as the three main strategies for answering our research question. In the remaining of this section we discuss the reasons of rejecting other approaches for this study.

Survey method could not be useful to gather required information in this study because enterprises do not have a common understanding of EA and SA definitions and their relationships. So that instead of conducting surveys with many companies or study various cases, we conducted interview with three experts who have worked for many different cases and have both academic and practical background.

We also could not apply case study since each organization selects limited strategies to develop security architecture, and we cannot investigate all the alternatives in a particular case. Thus it is crucial to classify relationships between EA and SA through a qualitative study before conducting a survey or study further cases.

3.2 Research Procedure

Finding answer to the research questions made us conduct a review on two key terms: enterprise architecture and security architecture. Therefore, we start our research by reviewing the materials related to history, concept, drivers, and frameworks separately for each term and also in relation with each other.

From one hand, the review on the history of EA frameworks like DoDAF, MODAF, TOGAF, NAF and Zachman showed us that each framework has different perception to security. Where some EA frameworks consider security as a view, while some others as a product or an artifact and still some others do not have a view nor a product rather they view security as a spirit of EA that must exists in all enterprise elements like human, technology and processes.

On the other hand, the history of security architecture showed us the reasons why this word came into existence. In fact, we realized that before SA there were other kinds of security management approaches but because the forms of threats have changed the view toward security also changed to a holistic view. Hence, SA came into existence. All these, made us to answer the question that what are the changes in threats that leads to a new security management approach? The answer to this question made us to have a review on current information security threats.

After going through the history of EA and SA separately, we started to analyze SA and EA together. By going through their history we managed to figure out how EA and SA get influenced by each other. For example, in our research we claim that SA is a subset of EA. History helped us to accept or reject our hypothesis by finding counterexamples.

At this stage, in order to gain a clearer picture of the subject, we constructed a template analysis based on different approaches that we found from literature review. In the following we will describe how we conduct a template analysis.

As mentioned earlier it was not possible for us to go through each and every article in the literature review, therefore we had to develop codes, these codes are the keywords that tends to show the possible relationships and trends of SA and EA. We just reviewed those articles and publications that are relevant to our keywords.

The keywords that we looked for in EA related articles, technical and practical documents were “Security” and “Security Architecture”. For example, one of the EA frameworks references was DoDAF document that were around thousand pages. Clearly we did not gone through the entire document; rather we just focused on security part and SA part of the document.

Beside enterprise architecture publications we also had to review security articles where our keywords were “Architecture”, “Holistic View” and “Enterprise Architecture” because of two reasons, first we wanted to know whether holistic view existed before and secondly how security is related to EA. The outcome of our template analysis presents a classification of EA and SA relationship throughout the history.

The Table 3.1 shows the steps taken in our research in relation with the three research strategies. Procedure of interview is described in section 3.4.

Table 3.1. Research Strategy & Research Method

Research Strategies	Research Method
Literature Review & Template Analysis	1. Review EA definitions, concept, challenges and drivers
	2. Review SA definitions, history, threats, different Information security management strategies.
	3. Produce an initial template of analysis
	4. Find and review articles that seeking for a holistic view as SA
	5. Classify the different approaches of SA
Qualitative Interview	6. Qualitative interview with EA experts to evaluate different approaches
	7. Interpret the findings

3.3 Literature Review

In our research we had a substantial body of literature on EA and SA. Where we searched for different keywords as a query such as “security and Enterprise architecture”, “security architecture and enterprise architecture”, “security in EA frameworks”, “drivers of EA”, “challenges of EA”,“EA history”, “ Enterprise Information Security”, “Information Security Architecture”, “enterprise security”, “enterprise security management”, “security standards”, “security threats”, “Enterprise network security”, “ Application security”, “IT security”, “Cyber security” “Enterprise software security”, “Security management architecture”, “ Information Systems Security”.

Our resource was mainly Lund University’s Libhub system and Lovisa that provides access to articles, journals, books, e-books. We have also used other databases such as Sciencedirect, ACM digital library, Emerald, IEEE and other databases that were introduced to us during library introduction section.

3.4 Expert Interviews

After finding different strategies from literature review, we needed to conduct an interview with EA experts who had experience in working with SA and different EA frameworks. The reason why we have selected interview is that each expert has experience of developing EA and SA in different contexts. In fact, this approach helped us as a shortcut to answer our research questions.

3.4.1 Interview Strategy

Our main method for data collection has been interviews. We have selected semi-structured interview in order to share a common understanding of EA and SA definitions and their relationship. Since it help us conduct interview in a more dynamic way rather than having structured questions answered one by one. This method provides both interviewer and interviewee with some degree of freedom for back and forth questions while the interviewer could control over the interview process and point it to preferable directions (Kvale & Brinkmann, 2009).

As Kvale and Brinkmann (2009) argued, it is important that an interviewer be knowledgeable enough in the area of research in order to fully understand the informants discussion and be able to find his answers in a back and forth conversation. The interviewer's skills and his knowledge and experience of subject could help us a lot in conducing, leading and analyzing the interviews. This was also beneficial in follow-up questions.

3.4.2 Design of Interview guide

Table 3.2 shows the interview guide where research questions and interview questions are mapped together.

Table 3.2. Mapping Interview Questions & Research Question

Research Questions	Interview Question
Q1: What are different strategies to develop Security Architecture in relation with Enterprise Architecture?	1. How security architecture could be developed independent of Enterprise Architecture?
	2. How EA artifacts could be used to develop SA?
	3. How the EA frameworks and methods could be used to develop SA?
	4. How security architecture could be developed as a part of EA?
Q2: What are the advantages and drawbacks of strategies of security architecture development?	5. What are the impacts of different strategies of SA development on effectiveness of SA (Business & Security alignment, integration…)?
	6. How do the different strategies of SA development affect efficiency of SA development?
	7. What is the difference between SA development strategies regarding practicality of outputs?
Q3: How EA frameworks can support enterprises to develop security architecture?	8. How EA frameworks could support security architecture development?
	9. Which components of EA (Methodology, framework, model, case tools, and reference model) are more important to support SA development? Why?

3.4.3 Selection of interviewees

To evaluate different strategies of SA we have conducted interview with three EA experts who have academic and practical background in both security and enterprise architecture fields.

Informant A: is an Enterprise Architect that is currently working as a CEO of a consulting company in the area of enterprise architecture. He has been the project manager of different EA projects.

Informant B: is a PhD candidate in computer science. He has been involved in different EA projects in the past 10 years as project manager. He has been assigned as the project

manager of developing Iran's national EA Framework. He is the author of several journal papers. He has also published a book which is a guideline for Iran's National Enterprise Architecture Framework (INEAF).

Informant C: is currently a PhD candidate and EA researcher. He has worked as an EA project manager for the last 6 years. He has also several published papers in this area.

3.4.4 Conducting and transcribing interviews

We started by sending emails to informants and made them aware of our research questions and goals. They acknowledged us for an online appointment. Because they were not available physically we had to conduct the interviews through synchronous communication such as oovoo, Google talk, and telephone.

The interviews with Informant A (IA) was made through Google Talk messenger that lasts for almost one hour while for Informant B (IB) was made through oovoo messenger that takes almost two hours, and the last interview with Informant C(IC) was made over phone and lasted for half an hour.

According to Kvale and Brinkmann (2009), audio recording is the most common way to save conversations. We did the same by using software applications "Audacity" and "myDicto" that helped us to record the informants' voice. It also frees the interviewer to focus on the topic and dynamics of interview. Audio recording helped us to rewind the tape to make sure that we have not missed any point.

3.4.5 Reliability and Validity

To achieve reliability we have tried to define and describe our objectives and processes as detailed as possible, so that every researcher could follow the same procedure. For example, in literature review and template analysis part we had clearly explained the way we selected the papers and documents. We have also mentioned the keywords that we used and the rationales for why understanding certain concept like EA and SA are necessary to answer our research question. We also used audio recorder during the interview to make the transcribing be as accurate as possible.

To enhance validity we have keep questioning ourselves if the interview questions and results could address our research questions. Also we have used triangulation strategy to ensure that data collected from different sources (Literature review, Interview and cases) about a fact are valid. We also found that it is important the result of interview be connected to literature review. Moreover, there might be the possibility of

misunderstandings when interpreting the interviews. To solve this issue we have tried to send the result of interview to informants for clarification.

3.4.6 Ethical issues & Research ethics

Normally ethics is required in a qualitative research when persons are involved in the research through survey, interview or experimental research (Kvale and Brinkmann, 2009). Although we did not conduct a face to face interview but ethics was still an important issue that needs to be considered. To achieve ethics in our work we assure the informants about the protection of their identities because the invasion of their identity may cause harm. We have also discussed the overall purpose of our research with informants and shared the interview questions and project objectives with them through email. During the interview we had make sure to clearly define the research intentions for informants. We also get the permission to record their voice and lastly we assured them for a copy of transcription and interview analysis before publicizing the results of their interviews.

3.4.7 Bias

In any research, the goal is to find the true answer to research question with a clear and open mind. So that bias, prejudice and preconceptions could not affect the outcome of our study (Backman, 1998; Qates, 2006 and Hammersley & Gomm, 1997). Norries (1997) believes that one way to avoid bias is to be “Self-critic” in all aspect of the research; therefore to avoid bias in our research we ask ourselves about the chosen approaches over and over again.

During the interview we have tried to not push informants to any direction, since the interviewer in our research has a valuable background in EA it was possible that his points of view affect the informants. To avoid that the interviewer just ask the questions and never explains his own understanding about different questions unless it was necessary or asked from informants for his explanation and clarifications.

4 Interview Analysis & Discussion

We have designed interview questions regarding research questions and our theoretical framework. In this chapter, the results of the interviews will be analyzed in three main categories based on our research questions. The answers of informants are analyzed and summarized in a table for each research question as follows.

4.1 Analysis of different strategies of SA development

According to the findings of literature review, there are different strategies to develop security architecture in relation with EA. A brief classification of informants' answers about different strategies is represented in Table 4.1. The codes of answers are defined as combinations of question number and informants' letter.

Table 4.1. Interview results about different strategies of SA development

Q1: What are different strategies to develop Security Architecture in relation with EA?			
Interview Questions	**Informant A**	**Informant B**	**Informant C**
1. How security architecture could be developed independent of EA?	SA could not be effectively developed independent of EA	SA could be developed through an independent process but it is impossible to define SA without EA elements	An independent SA could not be an architecture because of lack in holistic view
2. How EA artifacts could be used to develop SA?	Not only EA artifacts could help SA, but also the security concerns should be considered step by step in developing EA artifacts	EA dictates borderlines to SA in terms of where data goes throughout business processes and who access data	The data architecture and CRUD matrix could be used to define who can manipulate data
3. How the EA frameworks and methods could be used to develop SA?	The holistic approach of EA could be used in coordination of SA development	In Zachman Framework security concerns could be considered when data, process, and location interact & between different layers	The modeling and representing approach of EA could decrease complexities of SA
4. How SA could be developed as a part of EA?	SA could be developed as a reference model (e.g. LISI in DoDAF) concurrent with EA development	Security requirements can be defined along with EA specifications of data, process, system and technologies.	SA could be described by security models in relation with other EA artifacts

Due to widespread using IT in business processes, the vulnerability of business continuity against security incidents is steadily increasing (IBM, 2008). Also, by merging business and IT concerns, the complexity of information security concept have increased. The architectural view to the security would contribute simplicity of security analysis (C3). On the other hand, today by extending business processes and information flow beyond the traditional borders of organizations without a holistic approach to the information, process and data we cannot control information security (B2).

4.1.1 Independent Approach to SA development

Some enterprises define and develop their security architecture as an independent lifecycle from EA while SA originally is a subset of EA. The reason of this strategy could be the context of organizations. For example, if the responsible department of security is separated from IT department, the SA would be developed independent of EA. But architecture is a collection of descriptions of data, people, process, and policies, and without defining these elements security related decisions cannot be implemented completely in the enterprise (A1). The risk of this strategy is that the holistic view as the main point of architecture could be damaged because if security architecture does not consider process, data, people, and other aspects of enterprise, it will not have a holistic view to the security (C1). Also, if the security architecture development would be separated from EA, the security-driven decisions about system, network, and other layers of architecture would not be taken in time and correctly. In fact, there is a two-way relationship between EA and SA. However, the independent development of SA would not be a serious problem if the other architectures and elements of enterprise would be considered in SA development (B1). But in this case, SA could not affect EA effectively.

4.1.2 Using EA artifacts to develop SA

EA models and artifacts describe enterprise elements and can be used as a border to address security requirements. That is EA dictates borderlines to SA in terms of where data goes throughout business processes and who access data (B2). As Informant B pointed out the security requirements could be discovered and defined when different elements of enterprise interact with each other (B3). As an illustration, when a person want to access data, when a process manipulate data, or when data is distributed in different locations, security requirements can be discovered (C2). Furthermore, service, application and technology architectures could be used to identify vulnerabilities and design solution to enhance resilience and reconnaissance of IT services. However, according to informant C, in some cases EA artifacts do not cover SA needed information completely which could be improved by sending feedback to the EA team. For example, the location is an

important focus of security. If locations would not be described appropriately, it should be acknowledged to the EA team to improve EA artifacts.

As mentioned before, it could be a two-way interaction between EA and SA. That is the security requirements should be defined and delivered to EA team, and EA developers have to consider security requirements as design constraints (TOGAF, 2009; A2). Therefore, EA solutions will be designed securely by observing security requirements. On the other hand, in order to develop SA, security architects need information flow, business process models, definition of roles and responsibilities, blueprints of applications and infrastructures which are products of EA.

In order to clarify the strategy of using EA artifacts to develop SA, an EA development project which is managed by one of the researchers of this thesis, is discussed as an example.

Example 1: Developing EA & SA for an operational system

The project aimed to develop architectural models for a system based on DoDAF. With regard to importance of security, the organization decided to arrange a separate team for developing SA. The EA team was comprised of external enterprise architecture and internal technicians. Due to the fact that the organization did not have knowledge and experience of EA, the external EA professionals were assigned to the EA team. Also, the SA team included external security technicians and internal personnel. At the first step of the project, architecture definitions and expectations were reviewed, and the EA team found out that DoDAF has to be customized appropriate with expectations of the organization. Because DoDAF has not considered security architecture explicitly and organization wanted security architecture document as a separate artifact. In fact, they needed security architecture document to ensure compliance with security regulatory which was controlled by an external organization. The SA team which was managed separately negotiated with the organization and defined SA artifacts. Also, the project management board emphasized on close interaction between EA and SA teams. But out of the differences and disintegration of frameworks and methods of EA and SA, they had several challenges to interact. Finally, the EA team defined and delivered information flow models and matrix (OV-2 and OV-3), system exchange matrix (SV-6), system functionality (SV-4), model interfaces (SV-1), and communication model (SV-2) to the SA team. EA team described the EA artifacts in technical meetings with SA team, and SA team developed SA based on EA artifacts. But the problem of this project was that EA team just delivered their artifacts to the SA team and did not receive any feedback from SA team. In other words, the SA team could not play a considerable part in EA design decisions; therefore, the EA decisions on software architecture or network

architecture were taken based on operation, system and technology requirements while security requirements could affect selecting or rejecting some of alternatives. In addition, some of EA artifacts were changed during project, but the effects of these changes on SA artifacts could not be traced easily since EA and SA did not use a case tools. Therefore, the relationship between EA and SA team was a one-way road.

According to the above case, we can conclude that nature of the business and context could affect importance of security and shape organizational responsibilities of security. In this case, the sensitivity of security led to separating SA team from EA team. Also the regulatory compliance is an important factor in selecting strategy and method of SA. In addition, in this case, we could not integrate SA with EA completely due to the lack of integrated meta-model and case tools while SA and EA developed concurrently.

4.1.3 Using EA knowledge to develop SA

Since there is no universal definition for security architecture, EA definitions and previous knowledge about holistic frameworks and methods in EA field could be reused in SA development (C3). For example, EA holistic approach in IT and business alignment could be applied to coordinate SA development and align security with business (A3). Also, EA methods and techniques in change management could be used in tracing and managing changes of requirements and solutions. In addition, the meta-model and repository of EA can be used in security configuration management. Moreover, EA approach could be used as the means of communication between and among different security stakeholders. As an illustration, the Zachman EA Framework has been used to address security elements by several researchers (DeLooze, 2001; Henning, 1996; B3). A brief description of Delooze approach to develop SA using Zachman Framework is mentioned in the literature review chapter.

4.1.4 SA as a part of EA

According to the concept of EA as a holistic view of addressing concerns of stakeholders, security architecture could be developed a sub-set of EA, and Security requirements can be defined along with EA specifications of data, process, system and technologies (B4, C4). In fact, security requirements like data access regulations could be defined when information flow is being defined by enterprise architect. In other words, SA could be developed as other IT architectures and should be supported by EA frameworks. However, according to our previous discussion about SA and EA relationships, SA has a different nature compared to the other IT architectures, and it has been considered differently in EA frameworks. For example, SA could develop as a part of reference model like LISI (Levels of Information Systems Interoperability) or JTA (Joint Technical

Architecture) of DoDAF (2010) concurrent with other EA artifacts (A4). Also, TOGAF (2009) has defined SA as an independent but related concept to the EA. The ADM as the methodology of TOGAF has defined interconnections between EA and SA. One of the reasons of separating SA from EA in TOGAF is that the method of analyzing information flow and system functionality by security architects is different from enterprise architects. Security architects analyze situations in which system will not work, but enterprise architects investigate how system could work.

To describe different aspects of developing SA as a subset of EA, an EA development project which supervised by one of the researchers of this study will be explained as follows.

Example 2: EA development for a financial institution

A financial institution decided to change the main information system of institution out of supporting problems. The CIO of institution was working directly with the CEO of organization; therefore, with regard to the importance of mentioned system, CEO approved the EA development project of organization as a roadmap of change. An IT consulting company was selected to develop EA, and the EA team started project based on EAP methodology and Zachman Framework. The EA team aimed to develop all architectures such as business, application, data, network, storage, and security architecture; however, the main intended use of project was legacy transformation. SA document was one of the last documents delivered to the institution which means it was developed after data, application, and technology architectures. Since the priority of customer was not a holistic plan for security, the institution did not assign key security personnel in developing SA; in fact, the EA team developed SA based on other EA artifacts, trend of technology, and best practices in financial business area. Therefore, real security problems of the organization were not considered in developing SA. Finally, when SA delivered to the institution, security experts of institution did not accepted SA results and followed their traditional approach to the information security.

The above case shows that when an organization starts developing and using EA, the EA development team could not implement holistic approach in all sectors of enterprise in one step; however, the holistic approach of EA necessitates considering all aspects of enterprise, but it does not mean we can change traditional approaches rapidly. This case shows the reason EA has not covered all aspects of enterprise completely and is developing based on different situations.

By reviewing financial institution example, we can see the maturity level of IT management plays an important role in using proactive plans such as SA and EA. Also,

defining requirements and expectations of SA is an important factor to develop a practical SA. In addition, SA team has to be a combination of security experts of organization and external consultants to involve organization experts in developing their roadmap. In fact, EA approach has to be mature enough to extend holistic view into all enterprise sectors such as information security.

4.2 Evaluation of different SA development strategies

As we described in theory chapter, to evaluate advantages and drawbacks of each SA development strategy, we selected three main measurements: effectiveness, efficiency, and impact of SA development. According to the theoretical framework, to evaluate effectiveness of SA development we have considered common goals of SA development which have been generalized in literature review. The main goals of SA are holistic approach, security and business alignment, integration, change management, security requirements analysis, security cost reduction, compliance. We analyzed results of the interviews to evaluate effectiveness regarding above keywords. Also, to compare efficiency of different strategies we analyzed interview outcomes with regard to cost, time, and reusability of results. Finally, to evaluate impact of SA development strategies, we have investigated practicality of SA outputs of different approaches in implementing SA solutions in enterprise. The result of interviews about evaluation strategies is represented in Table 4.2.

Table 4.2. Interview results about evaluation different strategies of SA development

Q2: What are the advantages and drawbacks of different strategies to develop SA?			
Interview Question	**Informant A**	**Informant B**	**Informant C**
5. What are the impacts of different strategies of SA development on effectiveness of SA?	Security specialists used to focus on technological aspects of security, and EA could help them consider business requirements and align security with business	The security requirements could be analyzed by investigating the interaction between enterprise elements such as data, process, and people	Change management of SA could be easier when it develop based on EA. Also the business & IT alignment approach of EA could be used to align security with business
6. How do the different strategies of SA development affect efficiency of SA development?	EA artifacts could be used to capture and analyze security requirements, so the EA related strategies would be more efficient	Results of independent approach are not scalable to more enterprises. These are more useful in the context of certain enterprise but are not portable to others	Reusing EA knowledge and methods to develop SA could decrease time and cost of SA development
7. What is the difference between SA development strategies regarding practicality of outputs?	If SA develop based on EA, the SA solutions will be implementable through other IT architectures	Practicality of outputs depends on many factors such as management commitment and usability of SA outputs	The results of EA related strategies could be implement better through transition architecture of EA and EA change management process

4.2.1 Effectiveness of SA in different strategies

The effectiveness of SA is defined as how SA could realize goals of stakeholders. One of the main goals of developing SA is security and business alignment. On the other hand, EA includes useful methods to align business and IT; therefore, the strategy of using EA knowledge to develop SA could reuse knowledge of business and IT alignment to align security with business. Moreover, by reusing knowledge and tools of EA, security architects can develop an automatic repository for SA artifacts to integrate SA solutions and maintain SA. (C5)

The strategy of developing SA as a part of EA could also use the EA repository to develop and maintain SA. In this strategy, integration of SA artifacts with other enterprise models would be more effective because a unique anthology, methodology and case tools support both EA and SA development (C5). In addition, due to the two-way interaction between SA and other architectures, the security compliance requirements

will be effectively considered in design data, application, and technology architectures (A2).

Since independent approach is not related to a particular EA framework, the methodologies and standards of SA could be used by all enterprises in different contexts (Sherwood, 1996). In fact, enterprises in which security management is separated from IT management could use independent approach to develop a holistic plan for information security. But the risk of independent approach is that security specialists usually focus on technological aspects of security such as firewall, antivirus, encryption, and coding methods; therefore, in some cases the business requirements are not considered appropriately (A5).

The security requirements could be extracted and analyzed by investigating the interaction between other enterprise elements such as data, process, and people (B5). Therefore, by using EA artifacts to SA development or developing SA as a part of EA, security requirements of business will be completely captured and analyzed because EA artifacts describe all enterprise elements such as data, process, people, and location completely. In the independent approach, business requirements can be analyzed through interviewing business representatives (Sherwood, 1996), and risk of conflicting concerns of different interviewees threats SA consistency.

4.2.2 Efficiency of different strategies

Security is often considered an extra cost but with today growing global environment it can save data loss, competitiveness and hence brings in some value. But due to the fact that advantages of SA are intangible, generally estimating costs of SA development is so much easier than calculating benefits, and benefits could be described as cost-saving (PvIP, 2009). Therefore, in this part we will consider cost and time of SA development to evaluate efficiency of different strategies. According to informant B, strategies that pay more attention to details of more valuable data and processes are more likely to produce some value. These, however, are more expensive to develop and maintain.

In enterprises which have implemented EA, reusing EA knowledge to develop SA could reduce cost and time of SA development because according to the example 2 the architectural descriptions without participating enterprise experts would not be implemented, and transferring knowledge is always a time consuming and expensive process (C6). Also, if enterprises develop SA as a part of EA, the cost of integrating SA with EA will be saved.

Theoretically, SA could develop without underlying business and IT architectures, but this strategy will not be cost-effective because immediately, many principles have to be prepared for different possible scenarios that could make SA expanded and less useful for those people who need to work with SA (PvIB, 2009). In fact, if EA models could be used to develop SA cost and time of capturing business requirements and other needed information would decrease.

Strategies may be limited to general guidelines or be detailed through specification of processes, data access mechanisms and technologies. The former approach does not give out very particular results and is scalable to more enterprises. The latter approach results in particularly specific products. These are more useful in the context of certain enterprise but are not portable to others.

If enterprises use EA knowledge to develop SA or design SA as a part of EA, the SA building blocks will be more scalable and reusable because scalability is one of the basic principles of architecture; however, some independent SA development methods like SALSA (Sherwood, 1996) aimed modularity, scalability, and reusability of security solutions, but without architectural models and a logical holistic framework it is hard to develop reusable and scalable solutions for security.

4.2.3 Impact analysis of different strategies

The impact analysis of SA could completely be done after developing and implementing SA. But in this part, we will try to predict the practicality of different approaches of SA development considering potential factors of each strategy. Many parameters could affect actual impact of SA on security activities and solutions. Maturity of IT department, top management commitment, and usability of security solutions could affect impact of SA (B7). Also as we found out from example 2 that enterprises should have clear objectives of developing SA.

If enterprises develop SA as a part of EA, security concerns will affect data, application, and technology architectures through a two-way interaction. In fact, securing database, software, hardware, and network since early phase of design would be more effective, and helps enterprises put security requirements into practice through other EA artifacts (A7). In other words, planning security as an afterthought to cover security gaps of application and network is not an effective and feasible approach (Conkling et al., 2009).

In addition, if the SA implementation process would be integrated with EA transitional processes, the supportive disciplines of EA implementation such as change management,

budget planning, IT governance, and IT portfolio management will help enterprise to implement SA outputs effectively.

4.3 Analysis of EA Frameworks & SA

EA framework plays a significant part in characterizing EA. In accord with our literature review, each EA framework has considered security appropriate with the context of implementation and its own definition of security. It has always been an important question that how EA frameworks can support concerns of stakeholders effectively. The answers of informants to the role of EA frameworks in SA development and comparing different approaches in addressing security is extracted from transcriptions of interviews (Appendix1) and represented briefly in Table 4.3.

Table 4.3. Interview results about Role of EA frameworks in SA development

Q3: How EA frameworks can support enterprises to develop security architecture?			
Interview Question	**Informant A**	**Informant B**	**Informant C**
8. How EA frameworks could support security architecture development?	The security concerns should be considered step by step in developing EA artifacts, the framework should support this process	It depends on the context of enterprise, capability of EA team, and other factors. The chief enterprise architect should define a specific support the EA framework provides to SA for every specific enterprise.	The EA meta-model and repository could be used to develop SA, also EA has to provide all information needed for SA
9. Which components of EA (Methodology, framework, model, case tools, and reference model) are more important to support SA development? Why?	Addressing security architecture explicitly in EA ensures managers that security has been considered, but security should be considered in all architectures not just in limited artifacts DoDAF has covered security appropriately by LISI as a reference model and attributes of other EA products	All of the options could be the true in different contexts, it depends on the expectations of SA Approach of TOGAF is appropriate for business-oriented enterprises, DoDAF is suitable for mature and well-documented enterprises, FEAF is appropriate for a collection of small and medium enterprises which could cover security by common reference models and standards	Some artifacts of SA could be supported explicitly, but some of security concerns should be considered in development of other architectures

The EA framework is the main concept to address key concerns of stakeholders. But, according to our literature review, each EA framework has a particular strategy to address

security concerns because SA could not be defined universally and should be defined appropriate with the context of each organization. Therefore, there is no best position for SA in the EA frameworks, and the strategy of addressing security could be different in various contexts (B8). However, there are some general requirements of EA frameworks that have to be followed in each EA framework. First of all, the EA framework should support concurrent developing SA and EA step by step (A8). Second, the meta-model of EA framework have to support SA artifacts in order to integrate SA with EA (C8). Third security is not an afterthought like a shell that could cover gaps of none-secure solutions (Conkling et al., 2009). In fact, some of security requirements have to be considered in the initiating phase of design and development. For example, according to the Common Criteria standard (Internet 5), some of the security requirements of software development have to be considered since early phase of software development. Fourth, the expectations of SA and objectives of enterprise for a holistic view in security management should be defined clearly by enterprise.

Addressing SA explicitly is a strategy to increase visibility and separate-verifiability of security requirements to ensure managers that the security requirements are analyzed and considered appropriately, but by following this strategy, risk of ignoring security in other EA products will rise (A9, C9). Selecting the strategy of addressing security implicitly or explicitly in EA frameworks is responsibility of chief architect when she/he wants to customize EA framework based on expectations of stakeholders. There are several factors which could affect strategies of addressing security in enterprise such as expectations of stakeholders, expertise of EA team, context of developing SA, and etc. (B9).

Since different EA frameworks have developed by different organizations and adapted to their contexts, they have approached to the various strategies in addressing security. For example, DoDAF is a military framework that is developed and used to increase interoperability and integrity in US Department of Defense as a mature enterprise, and there are well-defined organizational procedures for SA development. Therefore, the security is not explicitly addressed in DoDAF, and just for integration of EA products with SA, security concerns are defined as attributes of other EA products (A9, B9). That is the reason DoDAF might not be a proper framework for the immature enterprises to develop SA as a part of EA as we found out from example 2. Also, the strategy of FEAF in addressing security by a reference model could be a useful approach to manage security concerns of small and medium agencies which could not invest on SA development by themselves (B9). In addition, since TOGAF has defined most of required disciplines to develop EA and integrate EA and SA, it could be used by business oriented organizations which have more freedom and independency to select different standards and approaches (B9).

The overview of EA frameworks' strategies in addressing security concerns is concluded in Table 4.4. In this table, different components of EA are defined in columns based on GERAM Framework (ISO/IEC, 2005). The main components of EA are reference framework, methodology, reference model, EA models, and EA tools. Cells of the table represent how each EA framework address security concerns explicitly in different EA components, and the empty cells show that there is no explicit evidence for addressing security by that component.

Table 4.4 shows that now EA frameworks do not support SA development completely. In fact, to develop security architecture, enterprises need a comprehensive methodology, security architecture descriptions and models, and a meta-model integrated with other EA artifacts. But according to the findings of this research, just FEAF and TOGAF consider security in methodology of EA; however, TOGAF has excluded developing SA from EA and just defined interconnections of EA and SA development processes. Also the security descriptions and models just defined by DNDAF; nevertheless, the security views of DNDAF just support limited parts of SA such as data elements, system data exchanges, and risk analysis. Other important parts of SA such as security policy, processes, and rules are not considered in DNDAF.

Table 4.4. Strategies of EA frameworks in addressing security concerns

Components / EA Frameworks	Reference Framework	Methodology	Reference Model	EA Models	EA Tools
DoDAF			CADM, JTA, LISI		The security attributes can be defined in EA case tools
DNDAF	Security Viewpoint is explicitly addressed			Secv-1 Secv-2 Secv-3	The security attributes can be defined in EA case tools
TOGAF		ADM contains relationships between EA & SA	ISM3		
FEAF		Security and privacy Profile	TRM & Security and privacy Profile		
Zachman (Heaney)	Security Abstraction is explicitly addressed			6 models in each perspective of Framework	

5 Conclusions

Thanks to the widespread use of IT in business processes and merging IT into business, firms are being more information-intensive. Therefore, they have to protect their information. Also, by extending information flows beyond the enterprise borders, providing information security has become a complex activity. Recent years, the architecture approach is considered to manage complexity of security. Since security is a growing concern of enterprise stakeholders, and EA is a means to address main concerns of stakeholders, security architecture was defined as a subset of EA. According to our findings, however security architecture is driven from EA but it is different from other sub-architectures such as business, application, data, and technology architectures. Applying standardization approach of EA to the security concept is not easily possible out of political, cultural, and social factors which influence security. On the other hand, EA has been created and developed by IT consultants in respond to customers' demand, and need for security architecture has been started approximately 10 years later. That is the reason SA has been separated from other sub-architectures, and enterprises follow different strategies to develop their SA. The first challenge against enterprises to develop SA is identifying possible strategies; therefore, our first question is defined as follows.

Q1: What are different strategies to develop Security Architecture in relation with Enterprise Architecture?

1. **SA development independent of EA:** SA could not have holistic approach if it would not be integrated with EA. However, SA could be developed through a separate process when scope of holistic approach is limited to the information security department or information security is not being managed by IT department according to compliance with security regulations.
2. **Using EA knowledge to develop SA:** Since SA has a holistic perspective on information security the EA frameworks, methods, repositories, and successful practices such as business and IT alignment, change management, and requirements analysis methods could be used in SA development. Especially in the cases that the knowledge of EA existed in the enterprise.
3. **Using EA artifact to develop SA:** security architects can use EA models to analyze security requirements and design integrated security solutions. In fact, EA dictates borderlines to SA in terms of where data goes throughout business processes and who access data. However, the more effective strategy is an active interaction between SA and EA to put security requirements into action through EA artifacts.

4. **SA as a part of EA:** if we define EA as a holistic view to the all aspects of the enterprise then SA could develop as a subset of EA. In this viewpoint, EA frameworks, methods, and transitional processes support SA development. Indeed, SA as one of the sub-architectures of EA could develop under the umbrella of EA. This strategy could be used by enterprises which have defined or implemented EA program.

After classifying SA development strategies, the enterprises need to evaluate different strategies from effectiveness, efficiency and practicality points of view. So that the following research question was designed to help enterprises select appropriate approach.

Q2: What are the advantages and drawbacks of strategies of security architecture development?

1. **Effectiveness:** the effectiveness of SA development strategies is evaluated considering to general goals of developing SA such as holistic approach, security & business alignment, integration, change management, security requirements analysis, security cost reduction, and compliance. According to our findings, by using EA knowledge and develop SA as a part of EA, security and business alignment could be inherited from EA to SA. Also integration of SA with other IT architectures would be more effective when EA artifacts could be used to develop SA. Since independent strategies are not related to a particular EA framework, the independent methods could be used to develop SA in enterprises which have to comply with special security regulations; however, in this case integration of SA with EA will not be achieved completely.
2. **Efficiency:** the most important differences between efficiency of SA development strategies deep rooted in reusing EA knowledge and artifacts and reusability of SA building blocks. Therefore, the most efficient strategy is developing SA as a part of EA because knowledge, artifacts and governance processes of EA could be reused in developing SA. Independent approach could be the most expensive strategy since business requirements have to be captured and analyzed as part of SA development. The efficiency of other strategies (using EA knowledge and using EA artifacts) would be at the interval of these two extreme approaches.
3. **Impact:** the practicality of SA outputs could be increased when SA is developing as sub-architecture of EA because supportive transitional processes of EA help SA implementing. Moreover, some of the security requirements can be implemented just through other architectures such as of software development, database, and network.

According to the results of evaluating different strategies, we can easily conclude that developing SA as a part of EA could be the most effective and efficient strategy if the

knowledge, maturity and context of enterprise would be appropriate. Therefore, an important question for enterprises which want to develop SA is how they should select or customize their EA frameworks to support SA development effectively and efficiently.

Q3: How EA frameworks can support enterprises to develop security architecture?

As mentioned before, security as a growing concern is addressed differently by EA frameworks. We have used GERAM framework as a meta-model of EA to investigate how SA could be situated in EA framework. According to our analysis, SA could be addressed in different parts of EA as follows:

1- **Reference architecture of EA:** security could be appeared as an independent viewpoint or view in the reference framework like DNDAF and E2AF. Since security is related to the all architectural layers such as business, data, application, and technology, SA usually crosses other viewpoints. Also if the reference architecture is Zachman framework, security could be considered as a new abstract after motivation as Heaney represented in his proposed framework. Representing security explicitly in the reference framework could facilitate SA development by focusing SA in some limited and explicit artifacts. Also this approach helps managers ensure that security compliance requirements are considered in EA. However, the risk of limiting SA to some artifacts is ignoring security concerns in other EA artifacts.

2- **Methodology of EA:** security development method could be included in the methodology of EA development. For example, TOGAF describes how EA and SA should develop concurrently; however, TOGAF defines SA as an external architecture.

3- **Modeling language of EA artifacts:** models are fundamental parts of EA, and modeling language describes how the EA description should be illustrated. If SA is addressed explicitly as a separated viewpoint, the modeling language of related artifacts should be described appropriately. Now there are some modeling languages to depict security requirements and solutions such as SecML and SysML. Also if the reference architecture considers security implicitly like DoDAF, security concerns should be defined as properties and attributes of other EA models. In fact, other languages of EA models should be extend to cover SA.

4- **Reference models of EA:** security concerns could be addressed in reference models of EA. That is common security requirements and related solutions could be defined as reusable patterns which could be extended to different context to solve similar security problems. The Security and Privacy Profile of FEAF and ISM3 of TOGAF are samples of security reference model.

5- **Case tools:** since architecture is a huge collection of models, developing and maintaining architectural models without automatic case tools is not possible. Case tools of EA development have to support methodology and modeling language of EA. Therefore, if security is an explicit viewpoint and includes some models and artifacts, the case tools of EA have to support developing SA models and integrating SA with other IT architectures. Also if security is addressed as an implicit concern, the case tools have to support meta-model of other artifacts.

However, there is no best strategy of SA development for all enterprises and there are some contingencies affect SA development, but there are some general points which have to be considered in all strategies.

1- All of the EA frameworks should support the integration of SA with EA by their meta-model.
2- They also should have a mechanism to define SA and EA concurrently; otherwise the security will be considered as an afterthought and cannot be integrated with other architectures.
3- Need for SA should be existed in enterprise and expectations of SA should be defined.

5.1 Future Works

According to our findings from expert interviews, enterprises follow different strategies for developing SA thanks to the both context and maturity level of enterprise. On the one hand, reasons of selecting particular strategy could be justify in terms of contingency factors. On the other hand, following SA development strategies could be explained based on evolution perspective. By reviewing our examples, we found following contingency factors affecting SA development approach:

1- **Nature of the business:** could affect importance of security and definition of security responsibilities in the enterprise.
2- **Regulatory compliance:** can affect strategies and methods of SA development. For example, Federal Agencies of US have to comply with NIST standard, so that they should use FEA reference models for security and privacy.

Also another hypothesis could be an evolutionary relationship between different strategies which justify how enterprises could achieve different levels of integration between EA and SA. According to our expert interviews, some of the factors to describe evolution from independent strategy to fully integrated strategy are as follows.

1- **Maturity level of IT management:** a mature IT management can lead to the proactive approach in IT management and integrating SA with EA.
2- **EA maturity level:** if the maturity of EA is in high level, knowledge of EA could be used in SA development. Also EA and SA can be integrated better thanks to the mature procedures for EA maintenance.

As a future work, both contingency and evolutionary factors would be investigated in order to realize which factors are more important to shape SA development strategy. The theory of this study could be a combination of contingency and evolution perspectives.

Also as another further work, the methodology of customizing EA framework to support SA development could be designed. To design this methodology, first of all, the important factors in SA development such as contextual parameters, maturity level of EA, expertise of EA team, and etc. should be identified. At the next step, different approaches and methods of customizing an EA framework should be reviewed. Finally, the designed method could be evaluated in a case study.

Appendix A: Glossary

ACM	Association for computing machinery
ADM	Architecture Development Method
ANSI/IEEE	American National Standards Institute/ Institute of Electrical and Electronics Engineers
AV	All View
BAE	British Aerospace Electronic Systems
BCE	before the Common Era
BS	British Standard
BSP	Business System Planning
C4ISR	Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance
CEO	Chief Executive Officer
CFO	Chief Financial Officer
CIA	Confidentiality, Integrity, Availability
CIO	Chief Information Officer
COBIT	Control Objectives for Information and related Technology
COMSEC	Communication Security
COO	Chief Operating Officer
CRUD	Create Read Update Delete
CSF	Critical Success Factor
CSI/FBI	Computer Security Institute/ Federal Bureau of Investigation
CTO	Chief Technology Officer
DNDAF	Department of National Defense and Canadian Forces Architecture Framework
DoDAF	Department of Defense Architecture Framework
E2AF	Extended Enterprise Architecture Framework
EA	Enterprise Architecture
EAP	Enterprise Architecture Planning
EISA	Enterprise information security architecture
ERP	Enterprise Recourse Planning
FEA	Federal Enterprise Architecture
FEAF	Federal Enterprise Architecture Framework
FOSs	Families of Systems
FY	Fiscal Year

GERAM	Generalized Enterprise Reference Architecture and Methodology
GMITS	Guidelines for the Management of Information Technology Security
IA	Informant A
IB	Informant B
IBM	International Business Machines
IC	Informant C
ICT	Information & Communication Technology
IEEE	Institute of Electrical and Electronics Engineers
INEAF	Iran's National Enterprise Architecture Framework
INFOSEC	Information Security
ISF	Information Security Forum
ISM3	Information Security Management Maturity Model
ISMS	Information Security Management System
IS	Info Systems
IS	Info Security
ISO	International Organization for Standardization
ISO/IEC	International Organization for Standardization/International Electrotechnical Commission
IT	Information Technology
JTA	Joint Technical Architecture
LISI	Levels of Information Systems Interoperability
MMS	Multimedia Messaging Service
MODAF	Ministry of Defense Architecture Framework
MOD	Military of Defense
NAF	Nato Architecture Framework
NATO	North Atlantic Treaty Organization
NIPC	National Infrastructure Protection Centers
Op	Operation
OV	Operational View
SA	Security Architecture
SANS	System Administration, Networking, and Security Institute SISS
SMS	Short Message Service
SOSs	Systems of Systems
SPP	Security and Privacy Profile
std	Standard
SV	System View
Sys	System
TAFIM	Technical Architecture Framework for Information Management

TEMPEST	Transient Electromagnetic Pulse Emanation Standard
Tech	Technical
TOGAF	the Open Group Architecture Framework
TRM	Technical Reference Model
TV	Technical View
UK	United Kingdom
US	United States
US-CERT	United States Computer Emergency Readiness Team

Appendix B: Interview Guide

As mentioned in the research methodology chapter, interviews conducted as semi-structured. The main questions asked in interview sessions are as below:

1. How security architecture could be developed independent of Enterprise Architecture?
2. How EA artifacts could be used to develop SA?
3. How the EA frameworks and methods could be used to develop SA?
4. How security architecture could be developed as a part of EA?
5. What are the impacts of different strategies of SA development on effectiveness of SA (Business & Security alignment, integration…)?
6. How do the different strategies of SA development affect efficiency of SA development?
7. What is the difference between SA development strategies regarding practicality of outputs?
8. How EA frameworks could support security architecture development?
9. Which components of EA (Methodology, framework, model, case tools, and reference model) are more important to support SA development? Why?

Appendix C: Transcripts

Interview ID: 1

A. General Information

Shahram= Researcher= R

General Information	
Interviewee Name	Reza Sani
Position	Enterprise Architect
Interview Date	2011-05-07
Interview Type	Through Google Talk
Time / Duration	Morning/ 60min
Referring abbreviation	Informant A=IA

B. Introduction and Warming up

Steps
1. Introduction
2. Describe the goals, aims and objectives of research
3. Assure the informant about confidentiality
4. Get the permission from interviewee to record the interview, and assure the interviewee that the interview transcripts, analysis and conclusions will be sent to him later for verification
5. Ask if informant has any general or particular information to add

C. Interview Transcript

1.	R	In your opinion, what is the importance of architectural view to the security?
2.	IA	If you look at to the security as an architect, then you will understand all aspects and elements of security. I mean holistic view of architecture help you get a big picture from security and

		can integrate it with other elements of enterprise.
3.	R	From your point of view, is security a concern in Enterprise Architecture?
4.	IA	Yes..
5.	R	According our findings, today enterprises have a holistic approach toward security architecture that integrates the whole enterprise layers ,strategic layer, system layer and technical layers
6.	IA	yea
7.	R	The result of our Template Analysis shows that, There are some researchers, who believe that security architecture is independent from enterprise architecture, and the reason for that is because of a holistic view, There are still some other researchers who believe SA is part of EA; would you tell us how do you see these two approaches? You think why an independent approach toward security architecture can be beneficial and what are the weak points of separating SA from EA?
8.	IA	I see the weak points in the real life implementation
9.	R	Could you explain more please? You mean SA in practice is not capable enough to be implemented?
10.	IA	See here…what are the things you deal with during an analysis phase? Aren't you dealing with procedures, rules and data?
11.	R	Yes.
12.	IA	So if you want to measure SA you have to find it in every rule, data and procedure…I have experienced in some projects of mine before that normally in real life there is no integration between information security elements in an enterprise…you think why is that?
13.	R	Isn't that because of the lack of a common language or a holistic view?
14.	IA	Well yea…but not exactly…the main reason is not because there is no common language...my experience proves me that some enterprises only view the security in physical and technological layer without paying much attention to processes and rules and data. I strongly believe that one could sense the security in EA with keep this in mind that we have to understand the relationship between different layers and their attributes in regard with security…
15.	R	You point out a very interesting issue while explaining your experiences, but different enterprise frameworks view security differently as an example DoDAF has no security view or artifact..
16.	IA	Very right.
17.	R	based on our research ,Some researchers believe that security should be seen everywhere, they also believe

		that an architect must have security at back of his mind while developing products But some like Netherlands or Canada military framework has a view or product in their architecture. What is Your analysis of different strategies within the framework of what you think of advantages and disadvantage of viewing SA as a view or product or not include any view like DoDAF?
18.	IA	This story was always more concerned with decision makers, they always ask questions like..Where is the security architecture? Why you don't have a security product?
19.	R	Don't you think limiting security to few artifacts or products might reduce the importance of security?
20.	IA	Definitely we can't limit security to just few products
21.	R	Would you explain more…do you mean that security must be viewed as a reference model for architecture?
22.	IA	Absolute
23.	R	Why do you think that a reference model for architecture is required for security?
24.	IA	Because the reference model architecture will be injected into the enterprise and in addition to that it starts to be complete in an iterative process..such as AV..LISI is an example of reference model architecture.
25.	R	As I understood you mean that in order to complete any framework like DoDAF, we don't really need to add security products for operation and system layers …make it easier to understand, do you mean that current EA frameworks like DoDAF are fulfilling the security issues although they don't have any security view or product?
26.	IA	Well I believe security is embedded in all the enterprise layers and products and if I want to do a project on SA I will add the security issues step by step as I am moving within EA and its products.
27.	R	My understanding from your point of view is that you believe security is merged in every step of planning, designing and implementing of EA products..
28.	IA	Absolutely, with this view you will satisfy the both approaches that you mentioned earlier and the result is a holistic approach toward SA
29.	R	Right.. Can I conclude that developing security artifacts might be good enough to cover certain security issues, but in order to cover the whole security concerns we need a reference model?
30.	IA	Yea, because at the end you will end up to architecture with secure products and an architectural reference model that guides the products.
31.	R	You think how the discussed different EA frameworks and methods could be used to develop SA?

32.	IA	What I see common among all the different frameworks and strategies is a holistic approach that tries to integrate different security elements, services and mechanism and align it with business. I see that the holistic characteristic of EA is strongly inherited in SA as well and could be used in coordination of SA development.
33.	R	How do the different strategies of SA development affect efficiency of SA development?
34.	IA	Efficiency is achieved when an enterprise tries to select the most appropriate strategy such that it avoids waste of time, money and energy in this case the EA artifacts could be used to capture and analyze security requirements, as a result the EA related strategies would be more efficient.

Interview ID: 2

A. General Information

Shahram= Researcher= R

General Information	
Interviewee Name	Ali Fatolahi
Position	Research in the EA field PhD Candidate
Interview Date	2011-05-07
Interview Type	OOVOO
Time/Duration	Morning/60min
Referring abbreviation	Informant B=IB

B. Introduction and Warming up

Steps
1. Introduction
2. Describe the goals, aims and objectives of research
3. Assure the informant about confidentiality
4. Get the permission from interviewee to record the interview, and assure the interviewee that the interview transcripts, analysis and conclusions will be sent to him later for verification
5. Ask if informant has any general or particular information to add

C. Interview Transcript

1.	R	…[] we start this section by explaining the different strategies and their advantages and disadvantages
2.	IB	What do you mean by Security Architecture? Do you mean IT security?
3.	R	No, I mean information security which is broader than IT
4.	IB	Does information security contain Information system security?
5.	R	Yes, it does
6.	IB	Do you see ISA in relation with ES. Are there any interfaces

		between ISA and ES or you just assuming information as something abstract to make it easier to understand?
7.	R	No, to be easier for us we are by now focusing on Information Security aspect only. We are not focusing on enterprise too much
8.	IB	But you are still trying to find a definition for ISA that is applicable in real world? And in practice? Isn't it?
9.	R	Well, yea..it is of course useful for practitioners to use our definitions and different approaches of ISA, because based on these document a reader could realize what specific approach they have toward implementing SA
10.	IB	So now I can see that you have an abstract view to information security and my suggestion to you is to keep this abstract view..otherwise your work is beyond a master thesis scope where you have to find interfaces between EA and IS
11.	R	Since now we are both clear, shall we start the interview questions? What is the importance of security architecture to enterprises?
12.	IB	Well it is so hard to answer this question since it is too broad
13.	R	Well we have tried to answer this question in literature review and we found that gaining a holistic view and depending heavily on IT infrastructure are the main reasons that makes SA important, but if you think there are any other points missed out, we are glad to hear them!
14.	IB	I see security architecture as a concern within any enterprise, maybe in the past you could make a ministry or a certain organization in charge for security and then claim that now everything is secure! But this doesn't work in real life and practice really! Now things changed such that security must goes along with every single process and data .make it short everywhere you find a piece of information it should be clear enough on the spot that to whom it belongs and how it should be secured? That is why Architecture comes in for example does the enterprise has the same security protocols with the data in hands of different persons? So who is responsible to define this? Who defines which information in an enterprise belongs to whom? Who must access and should not? So architecture can answer all these. When it shows the relation of different elements in an enterprise. From here we reach to the conclusion that security architecture is extremely intertwined with EA because where ever is an EA there is SA next to it. Although we call it as security architecture which sounds a standalone approach but in reality it is almost impossible to define SA without the elements of EA. That is why architecture is important…you could also argue that we had security before, but why not turns to Security Architecture? And the reason is

		because it is important that to map the relationship between the different elements of security within an enterprise..Today is impossible that you can't reach from one point to another point within an enterprise by using IT..so everyone and every unit are interconnected, so it is important that the defined security elements gather and map somewhere
15.	R	Thanks for your complete explanations, what is your view about the development of security architecture independent of Enterprise Architecture? What are the advantages and disadvantages of this strategy?
16.	IB	I don't see being independent as a problem really the problem is when it says SA is independent from EA..to me it sounds like SA doesn't necessarily come along with a specific EA rather it can come with any other EA, and there is no doubt that SA in itself is always merged with all the enterprise elements, even in an abstract way. But it is not necessary that it comes to enterprise always with EA or a specific EA
17.	R	That is very right, there is no doubt that all these elements, EA and SA are inherently interconnected. But now if you want to see from the EA that we have frameworks for, how do you define SA for that? You think how the formal EA the one that has many frameworks could help to define SA?
18.	IB	Take zachman as an example, he defines the relationships between different elements..Security is important when interconnections are happening. And another importance is that it define security between different layers as well, EA let me understand that what information in what process is created? In what Is read? and in which it is updated? Information security is another concern the comes shoulder by shoulder that says the information that need to be read in that specific process, who can read it? who can update it? who can create it? Which units of enterprise could do it? Is that information read by specific IT facility? Or is it allowed to copy or paste it? So I think EA show us the borders
19.	R	How do you evaluate the different strategies exist in different frameworks? For example DoDAF has the same view as you discussed earlier, while there are some EA frameworks that develop a view for SA, how do evaluate that? You think how these different approaches could have good or bad points in them?
20.	IB	Well, I guess this is mostly depends on the type of enterprise, seems like there are two approaches...in one approach security is too much involved with EA and another approach is that security is totally a separate view and the reason is quite obvious, for example DoDAF is developed for a very unique enterprise which is the military of USA. therefore the important thing that

		you have to understand here is that they defines security in DoDAF based on their own requirements therefore they believed that security is a concern for their own enterprise, maybe in other enterprises they have a security as a separate view because they still don't know how to apply it, or maybe their type and requirements of their enterprise is different from others. But over all I think that business decision makers need to consider that these two are always defined together.
21.	R	So you think the reason for different approaches is because of the context?
22.	IB	Yea..I think so. I have to add that context alone is not a matter; it also depends on different factors like how capable they are? How clear is the enterprise? How the security team knows about ..so my enterprise? Therefore my suggestion is that as an enterprise architect one must start with an inception where he gathers information about the context and requirements. So based on this then they can decide to view it as dependent, independent or what so ever! or define security components? This alone might be research question that how to reach to that guideline that allows us to understand the context and requirements much better? What is the procedure for applying security architecture in an enterprise? what are need things need to measured and studied?
23.	R	So you are saying that an architect must first find all the factors which could affect on which approach to choose?
24.	IB	Yea, at the end I am not saying that viewing security as an independent approach is something bad, if the architect feels so… it all depends on the context...for example imagine me and you have a company and we want to sell EA so in this case there is no need for SA and EA to be merged in a level that can't stay without each other! so we have to see them separately, later when we sell it to a company is time for us to connect SA with EA. So as you see in the example in such business SA is not merged with EA!
25.	R	Yea exactly you are saying that a business consulting company's concern is different from a military concern therefore they view security differently! So as an overall view since different EA frameworks compare Security issue differently, Do you think it is a good idea to compare these different approaches? Do you have any evaluation on security in different EA frameworks?
26.	IB	Well I am not really good in different frameworks; would you explain for me how each of these is viewing security?
27.	R	…
28.	IB	According to what you have explained for me I could say that TOGAF is more appropriate for Enterprises that are business oriented and private companies that can decide for their own, but

		the security view in DODAF is obviously showing that it is for a company with specific and predefined rules and no one is defining anything since everything is documented so in detail! So the way that DODAF views security is obviously showing that it is for a mature enterprise but in FEAF view toward security I could say that it has mostly a standard view so it is obvious that these standards are just some general guidelines for other enterprises and it is mostly like a checklist. Seems like this kind of approach is normally used for governmental enterprises or small businesses. So the budget here is a matter, I am trying to let you understand that not every enterprise in a country show have the same SA framework or approach. since it doesn't worth to invest equal amount of money for security for all businesses
29.	R	Now at this stage, after discussing the different strategies, you think how do these different strategies of SA development affect efficiency?
30.	IB	Well of course if different EA strategies do not existed, then the cost of SA development would increase to capture the business requirements since there is no single solution that fits all! So for enterprises to be more efficient there is a need to understand different strategies and select the one that is mostly match with business requirements.
31.	R	At last, you think what is the difference between SA development strategies regarding practicality of outputs?
32.	IB	I believe that there are many factors involved in the practicality of outputs in fact the output of each strategy is highly getting affected by the management commitment and usability of SA outputs.

Interview ID: 3

A. General Information

Shahram= Researcher= R

General Information	
Interviewee Name	Mohammad Ahmadi Achachlouei
Position	Researcher in EA filed, PhD candidate
Interview Date	2011-05-07
Interview Type	Telephone
Time/ Duration	Morning/30min
Referring abbreviation	Informant C=IC

B. Introduction and Warming up

Steps
1. Introduction
2. Describe the goals, aims and objectives of research
3. Assure the informant about confidentiality
4. Get the permission from interviewee to record the interview, and assure the interviewee that the interview transcripts, analysis and conclusions will be sent to him later for verification
5. Ask if informant has any general or particular information to add

C. Interview Transcript

1.	R	What is the importance of security architecture to enterprises?
2.	IC	It depends on your definition of SA!
3.	R	Well, Based on our review SA is a holistic view to security requirements and its solutions in relation with other elements of enterprise that considers all the policies and procedures, and our concern is on Information security
4.	IC	Well then I would say SA has the same concept as modeling in EA, and it is important because it works as a meta model and

		helps to manage changes and business alignment and security planning. But it is important to have the appropriate tools
5.	R	The result of our research shows that, There are different strategies for developing security architecture; some view it as dependent, while some as independent. What do you think about these different approaches? Their advantages and disadvantages?
6.	IC	Well I guess based on your definition ISA is a holistic view, the term "Holistic" is proving to me that SA is merged with EA otherwise SA by itself couldn't be holistic! The reason why SA is defined as a holistic view is because it is covering all aspects of an enterprise.
7.	R	In regard with previous question, one of the independent strategies in developing security architecture is developing SA based on EA artifacts, you think How EA artifacts could be used to develop SA?
8.	IC	You have to keep this in mind the first step in developing a security architecture is providing a clear map that defines who can manipulate the data within an enterprise, normally The data architecture and CRUD matrix are good options.
9.	R	You think how EA frameworks can support security architecture development better?
10.	IC	Well I guess it is important to understand that EA frameworks are meta-model and repository in nature ,therefore I could say that this characteristic of EA could be used to develop SA
11.	R	As I understood you are saying that EA is a meta model, what do you mean by that?
12.	IC	Well..are you agree that EA act as a model to specify information in an understandable language that is shared among different stakeholders?
13.	R	Yea..
14.	IC	Good, then we can use the same concept for developing SA, now referring back to your question , I would say that first we have to extract the characteristics of EA frameworks like meta-model and repository or any other to support security architecture development
15.	R	You think how EA framework should address security concerns (explicitly as a view or implicitly as background of other EA artifacts)? Why?
16.	IC	It depends, generally I can say that some artifacts of SA could be supported explicitly, but some of security concerns should be considered in development of other architectures
17.	R	How do you evaluate different EA approaches regarding security architecture?
18.	IC	I would say that Zachman framework could be used as a framework to develop security architecture. But DoDAF has

		not security artifacts explicitly therefore it is not suitable for beginners in SA development. and FEAF is a proper approach for a collection of organizations with common security concerns
19.	R	In regard with previous question, you think How SA could be developed as a part of EA?
20.	IC	Well, if an enterprise starts by developing SA as part of EA they could start by describing security models in relation with EA artifacts.
21.	R	At last, you think what is the difference between SA development strategies regarding practicality of outputs?
22.	IC	The results of an EA related strategy is strongly depends on the transition architecture of EA, how it is changed? In what extend it has changed? And the processes took into account for EA change management processes and the way it has been implemented.

References

Ahmadi, A.M., 2010. *The Concept of Enterprise Architecture in Academic Research*. Master. Department of Informatics. Lund University. Lund. Sweden.

Air force Doctrine Document, 2006. *Homeland Operations-Air force doctrine document*. [online] United State Air Force. Available at: <http://www.fas.org/irp/doddir/usaf/afdd2-10.pdf > [Accessed 25 April 2011].

Amer, H.S. and Hamilton, J.A., 2008. Understanding Security Architecture. *Proceedings of the 2008 Spring simulation multiconference (SpringSim '08)*,pp. 335-342.

Anderson, K., 2007. Convergence: a holistic approach to risk management. *Network Security*, 2007(5), pp. 4–7.

Anderson, J.A. and Rachamadugu, V., 2008. Managing Security and Privacy Integration across Enterprise Business Process and Infrastructure. *2008 IEEE International Conference on Services Computing*, 2008(2), pp.351-358.

Backman, J., 1998. *Rapporter och uppsatser*. Studentlitteratur, Lund.

Bayle, A.J., 1988. Security in open system networks: a tutorial survey. *Journal of Computers & Security*, 7(5), p. 523.

Bell, D., 2005. Looking Back at the Bell-La Padula Model. *21st Annual Computer Security Applications Conference* (ACSAC'05), 2005(15), p.351.

Bernus, P., Nemes, L. and Schmidt, G., (Eds.) 2003. *Handbook on Enterprise Architecture*. Springer Verlag.

Biba, K.J., 1977. *Integrity Considerations for Secure Computer Systems*. [online]. Available at: <http://oai.dtic.mil/oai/oai?verb=getRecord&metadataPrefix= html&identifier=ADA039324 > [Accessed 23 April 2011]

Blatchford,C.,2007.Information Systems Security and the Multinational Enterprise (2). *Journal of Elsevier Advanced Technology*,1996(3),pp.18-26.

Boh, W. and Yellin, D., 2007. Using Enterprise Architecture Standards in Managing Information Technology. *Journal of Management Information Systems*, 23(3), pp.163–207.

Brennan, J. J., Faatz, D., Rudell, M. And Zimmerman, C. 2004. Visualizing enterprise-wide security (VIEWS). *Computer Security Applications Conference*, p. 71-79.

Brewer, D.F.C. and Nash, M.J., 1989. The Chinese wall security policy. *Journal of Security and Privacy*, pp.206-214.

Brunnstein, K., 1997. Towards a holistic view of security and safety of enterprise information and communication technologies: adapting to a changing paradigm. *Computers & Security*, 16(3), pp. 208-208.

BSI (2002). Basic protection manual. Technical report, Bundesamt fuer Sicherheit in der Informationstechnologie.

Caralli, R.A., 2004. *Managing Enterprise Security.* [online] U.S. Department of Defense, Carnegie Mellon University. Available at: <www.cert.org/archive/pdf/managinges0412.pdf > [Accessed 25 April 2011].

CIO Council, 1999. *Federal Enterprise Architecture Framework*. [online] The Chief Information Officers Council. Available at :< http://www.cio.gov/documents/fedarch1.pdf> [Accessed 5 May 2011].

CIO Council, 2001. *Practical Guide to Federal Enterprise Architecture Framework*. [online] The Chief Information Officers Council. Available at: <http://www.gao.gov/bestpractices/bpeaguide.pdf > [Accessed 5 May 2011].

Clark, D.D. and Wilson D.R., 1987. A Comparison of Commercial and Military computer Security Policies, *1987 IEEE Symposium on Security and Privacy*, pp.184-194.

Clinger-Cohen Act, 1996. *Office of Managmenet and Budget*. [online] available at: < http://www.whitehouse.gov/omb/circulars_a130_a130trans4 > [Accessed 5 May 2011].

Conkling, W.R. and Hamilton, J.A., 2009. Suggested Improvements to the DoDAF for Modeling Architectural Security, *Proceedings of the 2009 Spring simulation multiconference (Spring Sim '09)*, San Diego, CA, USA.

DeLooze, L., 2001. *Applying Security to an Enterprise using the Zachman Framework*. [online] SANS Institute. Available at:<http://www.sans.org/reading_room/whitepapers/modeling/applying-security-enterprise-zachman-framework_367> [Accessed 1 May 2011].

Denning, P.J., 1991. Computers under attack: intruders, worms, and Viruses. *Journal of Computer*, 25(1), pp. 134-135.

Denning, E.D., 1999. *Information warfare and security*. Georgetown University Washington, DC. Addison-Wesley Longman Ltd.

Dlaminia, M.T., Eloffa, J.H.P. and Eloffb, M.M., 2008. Information security: The moving target. *Journal of Computers & Security*, 28(3-4), pp. 189-198.

DND/CF, 2010. *DND/CF Architecture Framework*. [online] Canada National Defense. Available at: < http://www.img.forces.gc.ca/pub/af-ca/vol-02/doc/vsv-vps-vol-2-eng.pdf> [Accessed 21 April 2011].

DoDAF, 2010. *DoD Architecture Framework Working Group*. [online] U.S. Department of Defense. Available at: < http://www.dod.mil/ > [Accessed 21 April 2011].

Ekstedt, M. and Sommestad, T., 2009. Enterprise Architecture Models for Cyber Security Analysis. *2009 IEEE/PES Power Systems Conference and Exposition*, ?(?), pp.1-6.

Ertaul, L. and Sudarsanam, R., 2005. Security Planning Using Zachman Framework for Enterprise. *Proc. of EURO mGOV 2005*. UK : University of Sussex, Brighton.

Ertaul, L., Braithwaite, T. and Bellman, B., *Enterprise Security Planning (ESP)*. [online] Available at:< http://www.m4life.org/proceedings/2005/PDF/15_S036EL-S13.pdf> [Accessed 25 May 2011].
Essmayr, W., Kapsammer, E., 1998. Enterprise-wide security administration. *Database and Expert Systems Applications, 1988 Proceedings Ninth International Workshop*, pp. 267-272.

Finkelstein, C., 2006. *Enterprise architecture for integration: rapid delivery methods and technologies*. Artech House.

Franke, U., Johnson, P., 2009. An Enterprise Architecture Framework for Application Consolidation in the Swedish Armed Forces. *13th Enterprise Distributed Object Computing Conference Workshops*, pp. 264 – 273.

Franke, U., Hook, D., Konig, J., Lagerstrom, R., Narman, P., Ullberg, J., Gustafsson, P. and Ekstedt, M., 2009. EAF2- A Framework for Categorizing Enterprise Architecture Frameworks. In *Proceedings of the 2009 10th ACIS International Conference on Software Engineering, Artificial Intelligences, Networking and Parallel/Distributed Computing* (SNPD '09), pp.327-332.

Gelbstein, E., 2006. *Information security for policy makers: what it means- why it matters- what to do about it?* [online] Available at: <http://www.unitarny.org/mm/File/Webinars/Unitar%20eg%20presentation%2030_08.pdf > [Accessed 25 April 2011].

Hammersley, M. and Gomm, R., 1997. *Bias in Social Research, Sociological Research*. [online]. Available at:< http://www.socresonline.org.uk/2/1/2.html> [Accessed 4 April 2011].

Hayashi, T., 2006. *Scheme for realizing total security in Information systems*. [online] Available at: <http://www.waseda.jp/assoc-cioacademy/pdf/hayashi.pdf> [Accessed 25 May 2011].

Heaney, J., Hybertson, D., Reedy, A., Chapin, S., Bollinger, T., Williams, D. and Kirwan, M., 2003. *Information Assurance for Enterprise Engineering*. [online] available at: <http://hillside.net/plop/plop2002/final/PLoP-2002-Heaney-7-22.pdf> [Accessed 1 May 2011].

Henning, R., 1996. *Use of the Zachman Architecture for security engineering*. [online]. Available at: <csrc.nist.gov/nissc/1996/papers/NISSC96/paper044/baltppr.pdf> [Accessed 1 May 2011].

Hensel, V. and Lemke-Rust, K., 2010. On an Integration of an Information Security Management System into an Enterprise Architecture. *2010 Workshops on Database and Expert Systems Applications*, pp. 354-358.

Hjort-Madsen, K., 2009. *Architecting Government: Understanding Enterprise Architecture Adoption in the Public Sector*. Ph.D., IT University of Copenhagen, Denmark.

IBM, 2008. *Take a holistic approach to business-driven security*. [online] IBM Service Management. Available at <http://www-03.ibm.com/systems/nz/resources/systems_ap_gmw14008_usen_00.pdf> [Accessed 15 May 2011].

(ISC) ², Security Transcends Technology .Case Study: Securing the Right Information Security Team.[online] Available at:< https://www.isc2.org/uploadedFiles/Industry_Resources/UBSFinal.pdf> [Accessed 14 May 2011].

Hillard, R. 2000. *IEEE-std-1471-2000: Recommended Practice for Architectural Description of Software Intensive Systems*. New Jersey: The Architecture Working Group of the Software Engineering Committee, Standards Department, IEEE.

Inmon, W., Zachman, J., Geiger, J., 1997. *Data stores, data warehousing and the Zachman framework, Managing enterprise knowledge*. McGraw-Hill.
Internet 1: Available at: <http://ist.psu.edu/newsevents/page2.cfm?intNodeID=100&intPageID=736&HeadlineID=358> [Accessed 26 April 2011].

Internet 2. Available at: <http://www.mod.uk/DefenceInternet/AboutDefence/WhatWeDo/InformationManagement/MODAF/MODAFDetailedGuidance.htm> [Accessed 26 April 2011].

Internet 3. Available at: < http://www.hawzah.net/per/magazine/os/009/os00908.asp > [Accessed 15 April 2011].

Internet 4. Available at: < http://www.opensecurityarchitecture.org/cms/definitions> [Accessed 18 April 2011].

Internet 5. Available at: <http://www.commoncriteriaportal.org/files/ccfiles/CCPART1V3.1R3.pdf> [Accessed 28 April 2011].

ISO15704, 2000. Industrial Automation Systems—Requirements for Enterprise-reference Architectures and Methodologies.

ISO/IEC, 2005. Annex C: GERAM, in ISO/IS 15704:2000/Amd1:2005: Industrial automation systems - Requirements for enterprise-reference architectures and methodologies.

Kaisler, S.H., Armour, F. and Valivullah, M., 2005. Enterprise Architecting: Critical Problems. *Proceeding of 38th Hawaii International Conference of System Sciences HICSS '05*, p. 224b.

Kallet, H. R., 2004. How to Write the Methods Section of a Research Paper. *Respire care*,49 (10), pp.1229-1232.

Tudor, J.K., 2006. *Information Security Architecture -An Integrated Approach to Security in the Organization*. 2nd ed. Auerbach Publications.

Kim, S., and Leem, C., 2005. Enterprise security architecture in business convergence environments. *Journal of Industrial Management & Data Systems*, 105(7), pp. 919-936.

Khayami, R., 2011. Qualitative characteristics of enterprise architecture, *Procedia Computer Science*, Vol.3, pp. 1277-1282.

King, R.W., 2002. How effective is your information systems planning?. *Long Range Planning*. 21(5), pp. 103-112.

King, N., 1998. Template analysis. in Symon, G. and Cassell, C. (eds.) *Qualitative methods and analysis in organizational research.* London: Sage Publications.
Kinser, P., 2007. Enterprise Security Architecture, *Information System Security Association*, [online] Available at :< http://www.issa-centralva.org/> [Accessed 15 April 2011].

Kurpjuweit, S. and Winter, R., 2009. Concern-oriented business architecture engineering. *In Proceedings of the 2009 ACM symposium on Applied Computing (SAC '09)*, pp. 265-272.

Kvale, S. and Brinkmann, S., 2009. *InterViews: Learning the Craft of Qualitative Research Interviewing*.2nd ed.SAGE publications.

Langenberg, K. and Wegmann, A., 2004. *Enterprise Architecture: What Aspects is Current Research Targeting.* [online] EPFL. Available at: < http://infoscience.epfl.ch/record/52669/files/IC_TECH_REPORT_200477.pdf > [Accessed 18 May 2011].

Lindström, Å., Johnson, P., Johansson, E., Ekstedt, M., Simonsson, M., 2006. A survey on CIO concerns-do enterprise architecture frameworks support them?. *Information Systems Frontiers* 8(2), pp. 81-90.

Lowman, T. and Mosier, D., 1997. Applying the DoD goal security architecture as a methodology for the development of system and enterprise security architectures. *Computer Security Applications Conference*, pp.183-193.

McGovern, J., Ambler, S., Stevens, M., Linn J., Sharan V., Jo K.E., 2003. *A Practical Guide to Enterprise Architecture.* Prentice Hall.

Michelle, S. O., Fu, H. and Zhu, Y. 2009. Enterprise information security architecture a review of frameworks, methodology, and case studies, *Computer Science and Information Technology*, pp. 333-337.

Mitre, 2004. Guide to the (Evolving) Enterprise Architecture Body of Knowledge, *Mitre Corporation*, [online] Available at: <http://www.mitre.org/work/tech_papers/tech_papers_04/04_0104/04_0104.pdf > [Accessed 5 May 2011].

Namkyu, L., Tae-gong, L. and Sang-gun, P., 2009. A Comparative Analysis of Enterprise Architecture Frameworks based on EA Quality Attributes, *2009 10th ACIS International Conference on Software Engineering, Artificial Intelligences, Networking and Parallel/Distributed Computing*, pp.283-288.

NIST and OMB, 2009. Federal Enterprise Architecture Security and Privacy Profile Integrated with the Federal Segment Architecture Methodology, V3.0. [online] Available at: <http://cio.gov/documents/FEA-Security-Privacy-Profile-v3-final-09-01-2010.doc> [Accessed 05 May 2011].

Niemann, K.D., 2006. *From Enterprise Architecture to IT Governance*, Friedr. Vieweg & Sohn Verlag.

Noran, O. and Bernus, P. 2009. Service Oriented Architecture vs. Enterprise Architecture: Competition or Synergy?. *Proceedings of the OTM Confederated International Workshops and Posters on on the Move to Meaningful Internet Systems (OTM '08)*, pp. 304-312.

Norris, N., 1997. Error, bias and validity in Qualitative Research. *Educational action research*, 5(1),p.172.

Oda, S. M., Fu, H. and Zhu, Y., 2009. Enterprise information security architecture a review of frameworks, methodology, and case studies. *2nd IEEE International Conference on Computer Science and Information Technology*, pp. 333-337.

Open security architecture (OSA) defines the security architecture. [online] Available at: <http://www.opensecurityarchitecture.org/cms/definitions> [Accessed 18 April 2011].

OMB , 2010. *Fiscal Year 2010 Report to Congress on the Implementation of the Federal Information Security Management Act of 2002*. [online] Available at: <http://www.whitehouse.gov/sites/default/files/omb/assets/egov_docs/FY10_FISMA.pdf > [Accessed 18 May 2011].

Peterson, G., 2006. Security Architecture Blueprint, *Archtech Group*, [online] Availabe at: <http://arctecgroup.net/pdf/ArctecSecurityArchitectureBlueprint.pdf> [Accessed 15 April 2011].

Luker, M. and Petersen, R. 2003. Computer and Network Security in Higher Education, *EDUCAUSE*, [online] Available at :< http://net.educause.edu/ir/library/pdf/pub7008j.pdf>. [Accessed 12 May 2011].

Porter, M. and Millar, V., 1985. How information gives you competitive advantage, *Harvard Business Review*, [online] Availabe at :< http://zaphod.mindlab.umd.edu/docSeminar/pdfs/Porter85.pdf > [Accessed 21 April 2011].

Pulkkinen, M., Naumenko, A. And Luostarinen, K., 2007. Managing information security in a business network of machinery maintenance services business - Enterprise architecture as a coordination tool. *Journal of Systems and Software*, 80(10), pp. 1607-1620.

PvIB, 2009. Security architecture: a new hype for specialists, or a useful means of communication?. [online] Available at: <http://www.pvib.nl/download/?noGzip=1&id=11542823>[Accessed 18 May 2011].

Rold, C.D., 2002. *Service Market: Technical Convergence*, Gartner Inc., Stamford, CT.

Rusell, D. and Gangemi, G.T., 1991. *Computer security basics. United States of America*, O'Reilly & Associates, Inc.

SABSA, 2008. *The SABSA Method*. [online] Available at: <http://www.sabsa.org/the-sabsa-method.aspx>. [Accessed 23 May 2011].

Schekkerman, J., 2004. *How to survive in the jungle of enterprise architecture frameworks*. 2nd ed. Trafford.

Schekkerman, J., 2004. Another view at extended enterprise architecture framework, *Institute for Enterprise Architecture Developments*, [online] Available at :< http://www.enterprise-architecture.info/Images/Extended%20Enterprise/E2A-Viewpoints_IFEAD.PDF> [Accessed 25 April 2011] .

Schekkerman, J., 2005. *Trends In Enterprise Architecture*. [online] Available at (Restricted to the members):< http://www.eaconsulting.com/Reports/Enterprise%20Architecture%20Survey%202005%20IFEAD%20v10.pdf> [Accessed 28 April 2011].

Scholtz, T., Byrnes, C. and Heiser, J., 2005. Establish an Effective Information Security Program, Part 1: Structure and Content, *Gartner*, [online] Available at (Restricted to the members): <http://www.gartner.com/DisplayDocument?ref=g_search&id=485572>

Scholtz, T., 2008. The Structure and Content of an Information Security Architecture Framework, *Gartner*, [online] Available at (Restricted to the members): <http://www.gartner.com/DisplayDocument?id=686311> [Accessed 21 April 2011].

Schöenherr, M., 2009. Towards a Common Terminology in the Discipline of Enterprise Architecture, *Service-Oriented Computing --- ICSOC 2008 International Workshops*, pp. 400-413.

Shariati, M., Bahmani, F. and Shams, F., 2011. Enterprise information security, a review of architectures and frameworks from interoperability perspective. *Procedia Computer Science*, Vol.3, pp. 537-543.

Shiozaki, T., Okuhara, M. and Yoshikawa, N., 2006. *Fujitso Enterprise Security Architecture*. [online] Fujitso. Available at: < www.fujitsu.com/downloads/MAG/vol43-2/paper01.pdf > [Accessed 23 may 2011].

Shah, H. and ElKourdi, M., 2007. Frameworks for Enterprise Architecture. *IT Professional, IEEE Computer Society*, 9(5), pp. 36 – 41.

Sherwood, J., 1996. SALSA: A Method for Developing the Enterprise Security Architecture and Strategy. *Journal of Computers and Security*, 15(5), p. 406.

Sowa, J. and Zachman, J.A., 1992. Extending and formalizing the framework for information systems architecture. *IBM Systems Journal*, 31(3), pp. 590 – 616.

Spewak, H.S., 1994. *Enterprise Architecture Planning: Developing a Blueprint for Data, Applications, and Technology*. John Wiley & Sons, Inc.

Stenzel, J., 2007. *CIO Best Practices Enabling Strategic Value with Information Technology*. John Wiley & Sons, Inc.

SANS, 2007. *The Ten Most Important Security Trends of the Coming Year*. [online] Available at :< http://www.sans.org/resources/10_security_trends.pdf> [Accessed 5 May 2011].

Tahajod, M., Iranmehr, A., Iranmehr, A., Darajeh, M.R., Branch, D. and Branch, S., 2009. A Roadmap to Develop Enterprise Security Architecture. *Journal of International Conference for Internet Technology and Secured Transactions*, (ICITST), pp.1-5.

Theoharidou, M., Kokolakis, S., Karyda, M. and Kiountouzis, E., 2005. The insider threat to information systems and the effectiveness of ISO 17799. *Computers and Security*, 2005(24), pp.472–84.

Thorn, A., Christen, T., Gruber, B., Portman, R. and Ruf, L., 2008. What is a Security Architecture? , *Information Security Society Switzerland*, [online] Available at: <http://www.isss.ch/fileadmin/publ/agsa/Security_Architecture.pdf> [Accessed 18 April 2011]

TOGAF, 2009. TOGAF Version 9, *The Open Group*, [online] Available at: (Restricted to the members) <http://www.opengroup.org/architecture/togaf9/downloads.htm> [5 May 2011].

Office of CIO of Ministry of Citizen's services in British Columbia, 2010. Information Security Architecture. [online] British Columbia : Office of the chief Information Officer, Information Security Branch, Ministry of Citizen's Services. Available at: < http://www.cio.gov.bc.ca/local/cio/informationsecurity/policy/ summaries/25_info_security_architecture.pdf >. [Accessed 08 June 2011].

Open Group, 2011. Open Information Security Management Maturity Model (O-ISM3), *The Open Group*, [online] Available at: (Restricted to the members) <https://www2.opengroup.org/ogsys/jsp/publications/ PublicationDetails.jsp?catalogno=c102 > [Accessible 5 May 2011].

Preez, D. W. D. and Pieterse, V., 2009. *Calculating Compliance Standard*. [online] Available at:< http://icsa.cs.up.ac.za/issa/2006/Proceedings/Full/32_Paper.pdf>. [Accessed 08 June 2011].

Raadt, B., Schouten, S. and Vliet, H., 2008. Stakeholder Perception of Enterprise Architecture. *Proceedings of the 2nd European Conference on Software Architecture (ECSA '08)*, pp. 19-34.

University of Sheffield, 2011. Template Analysis. [online] Available at :<http://www.sheffield.ac.uk/lets-evaluate/general/data-analysis/template-analysis.html> [Accessed 18 May 2011]

Wegmann, A., 2003. On the systemic enterprise architecture methodology (SEAM). *Proceedings of the 5th International Conference on Enterprise Information Systems*, Vol. 3, pp. 483-490.

Wikipedia, 2010. *Enterprise Information Security Architecture (EISA).* [online] Available at: <http://en.wikipedia.org/wiki/Enterprise_Information_Security_Architecture> [Accessed 24 May 2011].

Yang, M., Yuan, L. and Yang, Z., 2010. A discuss of computer security strategy models. *Proceeding of International Conference on Machine Learning and Cybernetics*, Vol.2, pp. 839-842.

Yoffie, D.B., 1996. Competing in the Age of Digital Convergence. *Harvard Business School Press Boston*, p.464.

Young, F.R. and Windsor, J., 2010. Empirical Evaluation of Information Secuirty Planning and Integration.*Communications of the Association for Information Systems*, 26(13), pp.245-266.

Zachman J.A., 1997. The challenge is change: A Management Paper, *Zachman International* ,[online] Available at: <http://www.zifa.com.>[Accessed 18 April 2011].

Zachman, J.A., 1987. A framework for information systems architecture. *IBM Systems Journal*, 26(3), pp. 276-292.

Zachman, J.A., 2001. Security and the 'Zachman Framework', *Enterprise Architecture Resources*, [online] Available at <http://www.hl7.org/documentcenter/public_temp_CC6EBF56-1C23-BA17-0C4C18F07D3164D9/wg/secure/Zachman%20on%20Security.pdf> [Accessed 1 May 2011].

Zachman, J.A., 2008. Zachman-three choices. [video online] Available at:< http://www.youtube.com/watch?v=iUKV3Clnoxw > [Accessed 29 April 2011].

Zuccato, A., 2002. *Towards a systemic holistic security management*. M.Sc. Karlstad University.