International Journal of Computer Applications (0975 - 8887)
Volume 174 - No.5, September 2017

Enterprise Architecture Frameworks: A Critique Review from a Security Perspective

Bandar M. Alshammari
Department of Information Technology
Aljouf University
Saudi Arabia

ABSTRACT

Enterprise Architecture (EA) provides organizations with an effective and efficient technique to manage their information technology (IT) systems. EA allows organizations to align their business needs with the required IT resources. Therefore, several enterprise architecture frameworks have been developed for several purposes depending on the organizations' objectives. These include achieving their vision in an effective approach and reducing complexity and cost of their systems. These frameworks also aim to make systems collaborate in the most efficient way. However, these EA frameworks pay little attention to endorsing security of the organizations. Specifically, they mostly focus on the organizations business needs and ignore the fact that securing their IT systems is crucial. This will eventually result in making these organizations at a higher risk of security attacks. This paper surveys the most common enterprise architecture frameworks in literature. It illustrates their objectives and the types of organisations deploy them. It also defines the principles that these frameworks aim to follow in order to achieve the organizations mission. The paper also surveys a number of security design principles that are critical for any organization to follow in order to protect it assets. Towards the end of this paper, a critique review of these frameworks and a suggested approach for applying security with regard to certain security design principles at an early stage of development.

General Terms

Enterprise Architecture, Information Security

Keywords

Enterprise Architecture Frameworks, Enterprise Architecture Principles, Security Design Principles, Security Metrics

1. INTRODUCTION

Enterprise Architecture (EA) is a recent technique that has emerged to serve the increasing need for managing complex IT systems and making these systems function in the most efficient approach [19]. The main objective of EA is to achieve organizations mission by reducing costs associated with their IT systems and align these systems with their business objectives [19]. Therefore, several EA frameworks have been recently developed to server these demands. Examples of common EA frameworks include: The Open Group Architecture Framework (TOGAF), Zachmann, and the Federal Enterprise Architecture [19]. These frameworks share the main objective of EA that is to align IT systems with the business. However, they differ in the type of organizations they are mostly applicable to. They also differ in the approach used to deploy these frameworks.

However, none of the existing EA frameworks provides a complete solution that addresses enterprises information security in a comprehensive approach. In fact, they pay little attention to security which could lead to an enormous impact on the business of the organization in case of security attacks. Many security attacks could be avoided if they are considered from an early stage of development. Therefore, the best EA framework is the one which endorses security from an early stage of deployment for a certain organization. This needs to follow specific EA principles which are defined with regard to the most important security design principles. These security principles must include the principles of the least privilege and reducing the attack surface size. Such framework must also define certain security metrics that can be followed in order to quantify the security of a given organization based on its EA artifacts at an early stage.

This paper reviews current research related to the area of the security assessment of organizations with respect to their enterprise architecture. In particular, it surveys the well-established enterprise architecture frameworks, relevant security design principles, security-related enterprise architecture principles, and security metrics. At the end, it provides a critique review of how existing EA frameworks should pay more attention to security in order to make organizations more secure in this regard.

2. ENTERPRISE ARCHITECTURE FRAMEWORKS

In recent years, information technology has changed business, but in many cases, that change is not aligned with the business strategy of an organization [4]. This has influenced organizations in a negative way and wasted many resources [4]. Enterprise Architecture provides the structure and control required to align an enterprises business operations and information technologies to support its business goals and strategies [18]. This section will survey the common enterprise architecture frameworks in the literature, including their specifications and principles. This includes surveying the four dominate enterprise architecture frameworks: the Zachman

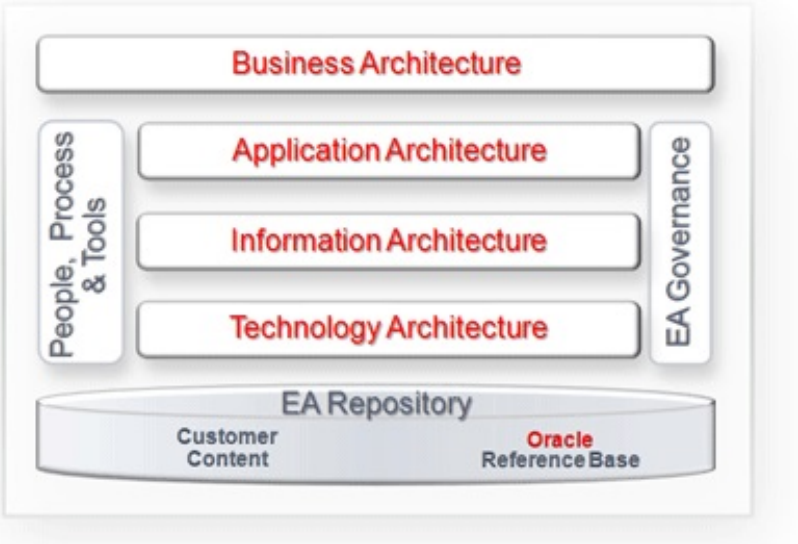

Fig. 1. Oracle Enterprise Architecture Framework (OEAF) [4]

Framework, the Open Group Architecture Framework (TOGAF), the Federal Enterprise Architecture (FEA), the Gartner Framework, and others. This section will also examine how information design principles can influence enterprise architecture frameworks.

2.1 Oracle Enterprise Architecture Framework (OEAF)

Oracle had developed its own EA in order to engage its customers in defining strategic plans which would increase the alignment between business and IT [4] (Figure 1). OEAF is defined to be a hybrid of other EA frameworks, and it is influenced by Gartner, FEA, and TOGAF [18]. Oracle claims that its EA framework is simple, practical, and prescriptive [4]. Furthermore, the OEAF has clear mappings to TOGAF and FEA [4]. The OEAF focuses on one principle, which is to create only the necessary structure for an organization that can be delivered on time and accomplishes the organizations business requirements [4]. Oracle claims that its EA framework has a great impact on improving the return on investment of the organization, since it improves the use of IT to execute the business strategy and uses IT resources more efficiently [4].

2.2 Federal Enterprise Architecture Framework (FEAF)

This framework was developed in May 2012 to serve the policy of the US federal CIO which was to increase the practice of EA in the US federal government [12]. It defines a number of principles for using EA to assist the US government federal entities make the best deployment of EA by eliminating duplicated resources and increasing shared systems [12]. Its outcomes include service delivery, functional integration, resource optimization, and authoritative reference. There are eight basic elements required by this framework: governance, principles, methods, tools, standards, use, reporting, and auditing [12]. The FEAF defines a number of general principles to ensure that potential investment and architectural decisions are weighed. These principles include Future Readiness, Investment Support, Shared Services, Interoperability Standards, Information Access, Security and Privacy, and Technology Adoption [12].

2.3 Ministry of Defense Architecture Framework (MoDAF)

This framework was defined by the UK Ministry of Defense to be capable of integrating various IT systems inside the ministry. It is recognized as an EA framework developed for supporting the ministry decision making and planning [10]. MoDAF consists of six viewpoints: the overall viewpoint, operational viewpoint, system viewpoint, technical viewpoint, standard viewpoint, and acquisition viewpoint [10]. Currently, there are a number of organizations that uses the MoDAF, including the Thales group, BAE systems, and Avolution [1]. Some other organizations have developed their own enterprise architecture that is identical to MoDAF except that they have added minor enhancements to the framework, such as the NATO architecture framework (NAF) [1].

2.4 US Ministry of Defense Architecture Framework (DoDAF)

DoDAF is a recent framework that was developed for defense systems by the US Department of Defense [11] (Figure 2). It classifies architectures based on four views: the system view, the technical view, the operational view, and the overall view [11]. It is claimed that many of the recently developed enterprise architecture frameworks were derived from DoDAF, including TOGAF, Zachman, and Gartner [1].

2.5 Gartner

Gartner states that EA should always be consolidated from top to bottom, and hence when developing an EA, business should be considered first, then information, applications, and technology [16]. One of the key steps in Gartner framework is to consolidate future state architecture before the current state is documented. This is then followed by other outcomes, such as actionable road map and gap analysis. Gartner states that most of the effort should be spent

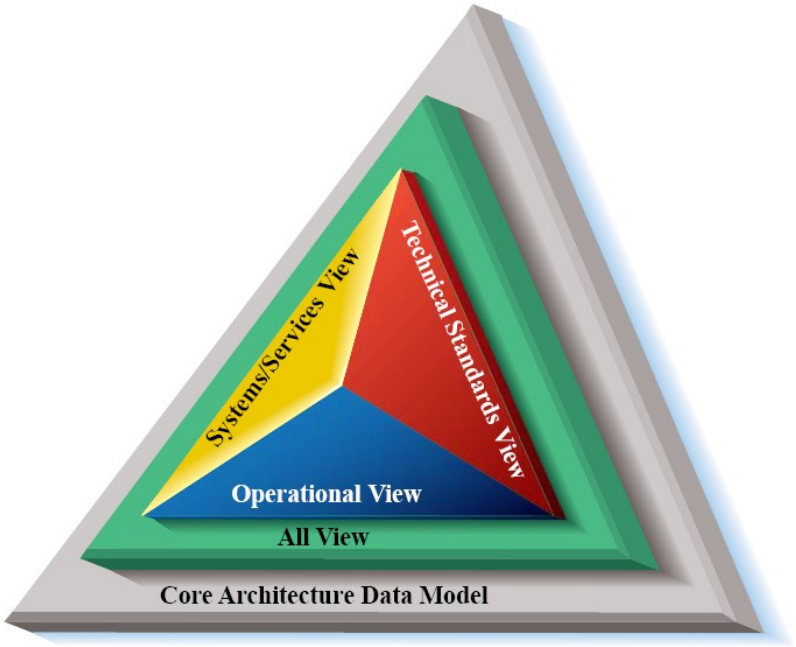

Fig. 2. US Ministry of Defense Architecture Framework (DoDAF) [11]

on communicating, strategizing, leading and governing, while architecting should receive little attention [16].

2.6 Queensland Government Enterprise Architecture (QGEA)

The QGEA framework developed by the Queensland government CIO [14]. It is composed of a several policies and documents that aim to direct the entities within the Queensland government to improve the compatibility and reduce the cost of its IT systems [14]. Consequently, the QGEA frameworks main objective is to be able to organize organizations' resources (i.e., processes, information, and IT infrastructure) [14]. It also needs to achieve the required business outcomes and technology integration by producing a set of policies and technical principles for the organization. The QGEA framework is divided into three elements: context, artifacts, and portfolios [14]. These elements have a link between each of them that represents a key strength of this framework [14]. For instance, portfolios are analyzed using context, and their alignment measures the artifacts effectiveness. The context element is the one responsible for the organization and navigation of the QGEA. It consists of five layers: four of them are horizontal including business, information, application, and technology, while the fifth one is vertical, representing the information security layer [14]. The outcome of this element is five frameworks, each of which is related to a specific layer [14]. For example, the business layer directs to the business process classification framework, but the information layer directs to the information classification framework, and so on. The artifact element provides the mechanisms and supporting tools for guiding the development and management of the government services, processes, information, applications, and technology infrastructure, which can ultimately help to establish the entire EA of the organization [14]. The portfolio element of the QGEA framework aims to document the current state of the organizations resources and initiatives and to plan the future state of the organization based on its resources and initiatives [14].

2.7 Zachman Framework

John Zachman defines the Zachman framework as a "logical structure for classifying and organizing the descriptive representations of an Enterprise that are significant to the management of the Enterprise, as well as to the development of the Enterprises systems" [21]. Its main goal is to provide a logical structure for organizing the enterprises design artifacts. This can eventually help the enterprises managers to make decisions in a very effective manner. It consists of a 6x6 matrix. The columns represent six aspects of the enterprise that can be described or modeled: the data, function, network, people, time, and motivation [21]. The rows in the Zachman framework represent six viewpoints from which the aspects can be described: the scope, business, system, technology, detailed representation, and functioning enterprise viewpoints [21]. The intersection between each column and row forms a cell that represents an aspect of the enterprise modeled from a particular viewpoint [21]. Each cell can then be selected by an enterprise architect to serve a specific purpose [21]. This selection ability represents an advantage of the framework since it allows architects to focus on a specific aspect of the system instead of looking at the system as a whole without losing any details of the entire system. This means that this framework allows architects to look at an enterprise system in an organized way, which helps in analyzing the system as a whole [21].

2.8 The Open Group Architecture Framework (TOGAF)

TOGAF is derived from the US DOD framework, and its main objective is to improve the business efficiency of organizations by

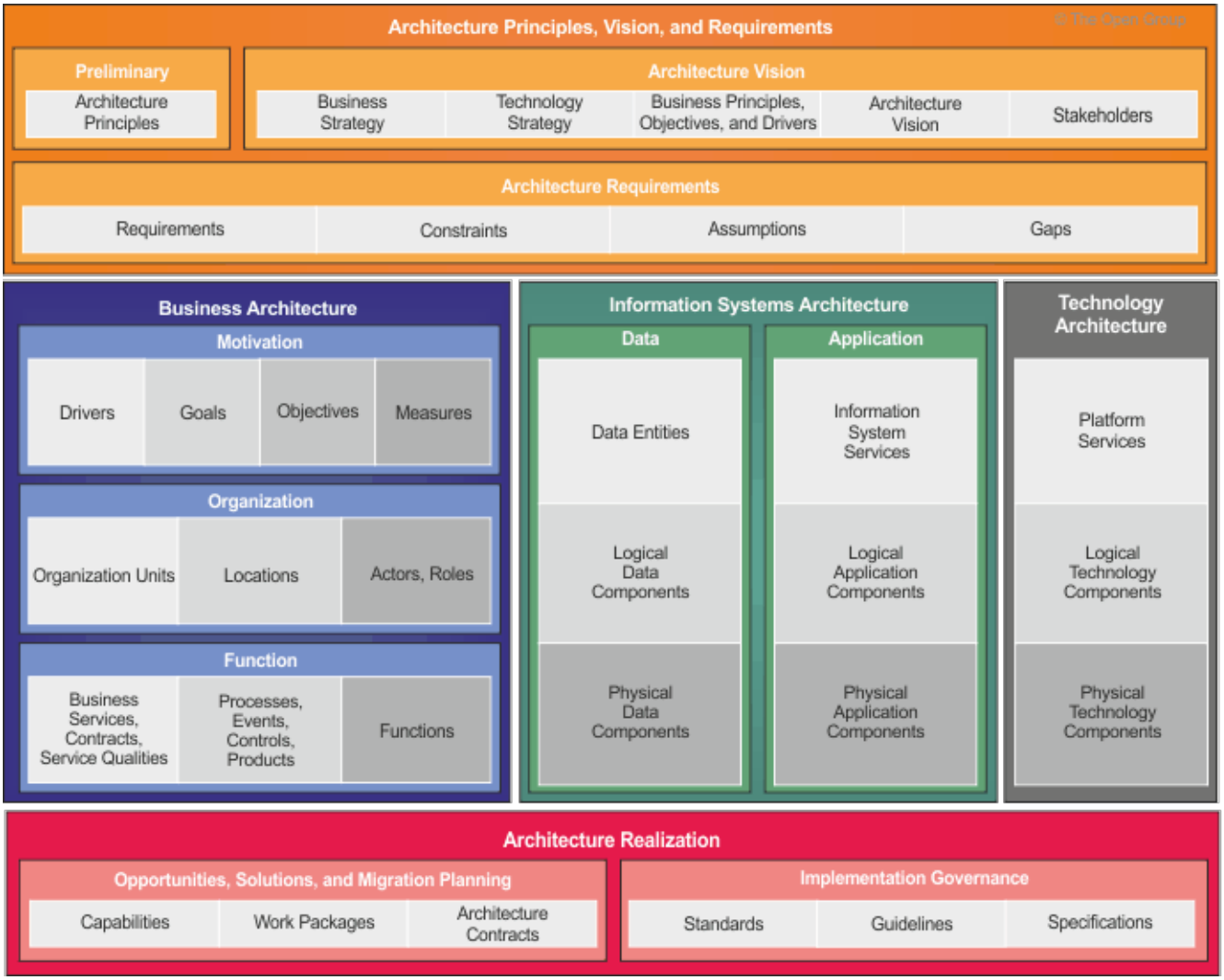

Fig. 3. The Open Group Architecture Framework (TOGAF) [19]

providing them with a methodology that allows them to do that [19] (Figure 3). This can be acquired by utilizing resources in an efficient approach to have a greater result on the business ROI. Furthermore, TOGAF is capable of providing simple implementation, and excellent alignment between business and IT [19]. The framework consists of six components: the architecture development method (ADM), architecture content framework, reference models, ADM guidelines and techniques, enterprise continuum, and enterprise capability framework [19]. The ADM represents an important component, as it is responsible for developing the enterprise architecture by addressing the business requirements [19]. It is an iterative process that comprises eight phases. Phase one is responsible for creating the architectural vision and validating the business context [19], which includes defining the main business and technology strategies. Phase two of the ADM is responsible for creating the business architecture, which includes defining the business goals, services, and processes [19]. The main responsibility of phase three is to develop the information system architecture, which is divided into two parts [19]. One part is related to the data of the system, while the other part is related to the enterprises applications. Phase four is responsible for creating the technology architecture, including the platform services, logical technology components, and physical technology components [19]. The architecture content framework details the inputs and outputs that are required by the ADM in order to execute. Therefore, it should be used in parallel with the ADM. There are a number of artifacts that are produced across the TOGAF ADM cycle. These artifacts are categorized into three categories: catalogs, matrices, and diagrams. For example, in phase three of the ADM process, which is the data architecture, these artifacts include the Data Entity/Data Component catalog, the Data Entity/Business Function matrix, the Application/Data matrix, the Conceptual Data diagram, the logical Data diagram, the Data Dissemination diagram, the Data Security diagram, the Data Life-cycle diagram, and Data migration [19].

To sum up, it can be concluded that all current EA frameworks share the same purpose, that is to create an EA that increases the alignment of business and IT resources. This goal can lead to re-

ducing complexity of systems and utilizing resources within the organization in an efficient approach.

3. RELEVANT SECURITY DESIGN PRINCIPLES

Several works have defined a number of important design principles that need to be followed in order to develop more secure systems, including the works of Saltzer and Schroeder [15], Bishop [3], and McGraw [9]. Such principles provide guidance for system engineers to improve the quality assurance of systems and therefore improve system security. Since there are many defined security design principles in the literature, the focus here is on the principles that are most applicable to the scope of this project. Here, the goal is to measure security statically, based on the enterprise architecture artifacts. Therefore, security design principles that influence security with regard to an enterprises static architecture need to be examined. This section reviews some of the most common security design principles.

3.1 Secure the Weakest Link

The main aim of this principle is to focus on securing the weakest parts of the system since many hackers prefer to attack simple parts of systems [9]. It is known that the systems weakest parts are often the parts which rely on human intervention by, for instance, administrators, users, and technical support staff [20].

3.2 Economy of Mechanism

The main objective of this principle is to increase security by making systems' security mechanisms simple in a way that doesnt weaken them [3]. Therefore, many approaches suggest reusing known good quality components of the system [9], which shows one way of adhering to this principle. This principle is important during the system design process because unnecessary information or control flow paths could result from an overly complex design [15]. To make the design simple, known components of good quality should be reused in the system whenever possible [20]. However, those parts of the system whose security mechanisms are unknown should be inspected carefully to determine whether to use them or not [3].

3.3 Reduce the Size of the Attack Surface

This principle is a very common principle that aims to reduce the number of components that can be accessed by outsiders [7]. There are several approaches to reducing such components. A common approach described by Howard [7] suggests reducing the amount of running code by turning off any unnecessary features of the system. Another approach is to minimize the number of entry points in the system that can be accessed by entrusted users [7].

3.4 Least Privilege

This principle is described as allowing programs and users to complete a certain job with the least possible privileges [3]. This principle is also known as "the need to know" [15]. It aims to minimize the number of interactions between privileged entities in a given program which would minimize lost cost in case of an attack [15]. A similar principle to the least privilege is the principle of the least authority. It recommends that objects that have access to certain parts of a system should not have access to other parts of the same system [17].

3.5 Defense in Depth

This principle requires backing up each security layer in any system with another security layer [6]. Therefore, once a certain layer is hacked, there is another one in place to protect the system, hence achieving a higher level of security.

4. ENTERPRISE ARCHITECTURE PRINCIPLES

Principles are widely used in organizations to set the rules and guidelines for how they can achieve their missions. Therefore, organizations can define a set of principles that are usually related to different domains or levels within the organization. These principles are divided into two domains: one domain is related to the enterprise, while the other defines principles with respect to the architecture [19]. The first domain defines a set of high-level principles for the enterprise to support the enterprises decision-making at a higher level [19]. The second domain is related to setting rules for the architecture development process of the enterprise [19]. These rules are in turn concerned with setting rules for deploying IT resources and assets within the organization. They also set underlying guidelines for making decisions that are related to the enterprise IT. Therefore, it can be said that these rules are related to a lower level of the organization. Since this project is related to the enterprise architecture, this paper only considers those principles that apply to the architecture domain [19].Enterprise architecture principles are defined by the enterprise architect in consultation with the organizations main stakeholders [19]. They must be defined in a way that ensures the alignment of IT and business strategy to ensure that the enterprises main vision is achieved [19]. The enterprise architect needs to consider a number of elements with regard to the organization while developing its enterprise architecture principles. These elements include the enterprises mission and plans, its strategic initiatives, its external constraints on current systems, and the emerging industry trends [19].

There are five properties that can distinguish a good principle from a poor one. These five properties are as follows: understandability, completeness, robustness, consistency, and stability [19]. Any principle that does not adhere to these properties is poorly defined and will definitely lead to poor decision making in terms of the organizations future planning. For each defined principle, its statement, rationale, and implications must also be defined [19]. This definition process can give a proper understanding of the main objectives and use of the project.

In the literature, enterprise architecture principles are divided into four types. Each type contains a list of principles that belongs to a specific domain of the four major EA domains (i.e., business, information, application, and technology) [19]. For example, the set of EA principles that are related to the business domain include the following: Maximize Benefit to the Enterprise, Information Management is Everybodys Business, Business Continuity, Common Use Applications, Service Orientation, and IT Responsibility [19]. Information domain principles include the following: Data is an Asset, Data is Shared, Data is Accessible, Data Trustee, and Data Security [19]. Examples of principles that belong to the application domain are Technology Independence and Ease-of-Use [19]. Finally, Technology domain principles include Interoperability, Control Technical Diversity, Responsive Change Management, and Requirements-Based Change [19].

Another work was conducted by University of Birmingham to build its EA. It stated a number of principles that suit the universitys main business strategic objectives. For example, the principles that are defined for the business domain include innovation, agility, value,

and priority [5]. The data domain principles consist of confidentiality, integrity, availability, accountability, dependability, and the information life cycle [5]. The application domain principles include reusability, plug and play, interoperability, system life cycle, coherence, and hiding [5]. Finally, the principles for the technology domain are defined: simplicity, standardizing, rationalizing, tiering, monitoring, green, virtualization, and capacity planning [5].
Further work was conducted by the University of Saskatchewan to define the principles of its Enterprise Architecture. The business domain principles include reducing duplication, maximizing value, and continuous improvement [8]. The data domain defined principles that were similar to the ones defined by the University of Birmingham: data secrecy, ease of access, and data sharing [8]. The application domain principles included technology independence, ease of use, simplicity, and reusability [8]. The technology domain enterprise architecture principles included requirement-based change, responsive change management, control of technical diversity, and seamless integration [8]. Similarly, the EA of the Washington University in St. Louis (WUSTL) defined a number of principles that are applicable to the four domains [13]. For example, the business domain principles are mostly concerned with the business processes, and hence its principles for this domain consist of business processes optimization, efficiency, effectiveness, and reusability [13]. The data domain principles are concerned with data confidentiality, availability, accountability, and accessibility [13]. The application domain principles are related to the independence of systems, reusability, integration, standardization, and alignment with the business of the university [13]. Finally, the technology domain principles are concerned with customization, availability, scalability, and the availability of information technology infrastructure [13].
The EA of the Norwegian Higher Education sector takes a different approach in terms of defining its enterprise architecture principles [2]. Instead of defining a list of principles for each domain, it defines a broad set of principles. It then examines their consequences, references, interdependence, and impact on each of the EA domains [2]. For instance, it defines a principle that is called "Accessibility". It then explains that the main purpose of this principle is to make the enterprise services available, easily found, and usable [2]. The consequences of this principle are then defined for each domain of the enterprise architecture. The consequences on the business domain include making sure that services are available and user-friendly and planning to automate the organizational processes [2]. The consequences of the accessibility principle on the data domain are defined to include the following: data are easily accessible by every authorized person at anytime from anywhere, worldwide [2]. The document states a number of consequences of this principle on the application domain, including the following: making all applications available, user-friendly and compliant with universal design principles [2]. Finally, the document states a number of consequences of the accessibility principle on the technology domain, including making the infrastructure of the organization platform-independent in order to be accessible by services from other platforms [2]. Other principles defined by the enterprise architecture of the Norwegian higher education sector include service orientation, security, transparency, flexibility, and scalability [2].

5. DISCUSSION

It can be seen that existing EA frameworks dont consider security as a major requirement. These frameworks mostly focus on making organizations IT systems align with the business in the best effective way. This is usually done by not taking security of that organization into consideration. In fact, security receives little attention or in many cases it is ignored till a very late stage. Security is a crucial requirement for all types of organizations, and the best EA is the one which takes security into considerations from an early stage. Therefore, there is a necessity for developing an EA framework that considers security as a major requirement for any organization. Such framework can be developed in the same way as other EA frameworks such as TOGAF or Zachmann. However, security needs to be applied to every level of development for that framework. This can result in developing a complete EA solution that considers all aspects of securing assets of any organization. This can also lead to protecting organizations assets from being attacked or exposed by unauthorized parties in an effective approach. Furthermore, such framework must consider the most important security design principles. Such principles are crucial for any organization to follow in order to be secure from unauthorised attacks. This can be achieved by defining enterprise architecture principles with regard to these security design principles. These EA security-related principles will provide guidance for EA architects when developing an EA.
Moreover, this new framework must provide a quantifiable approach that allows EA architects to measure security of any organization based on its EA artifacts. This can be achieved by developing specific security metrics that are applicable at all levels of EA design artifacts in order to measure security of any EA at an early stage of development.

6. CONCLUSION AND FUTURE WORK

This paper has surveyed the most common enterprise architectures frameworks in the current literature. It has also showed their definitions, principles, and how they are applied. The paper has also surveyed the most important security design principles that are applicable to the enterprise architectures. However, it has been shown that these existing EA frameworks dont consider security seriously, which in fact needs to be addressed when developing an EA for any organization. Therefore, there is a necessity for future work to develop an enterprise architecture framework that takes into consideration security in every aspect of the EA development for any organization. Therefore, it is concluded that the most effective EA framework is the one which endorsed security in all of its development stages. Such framework must follow certain architecture principles that satisfy specific security design principles. It must also provide a quantifiable approach for measure security of the organization based on its EA artifacts at any level of development.

7. REFERENCES

[1] A. S. Alghamd. Evaluating defensearchitectureframeworksforc4i system using analytic hierarchy process. *Journal of Computer Science*, 5(12):1075–1081, 2009.

[2] H. Bergh-Hoff, C.-F. Srensen, J. E. Garshol, B. H. M. Jakobsen, G. M. Vangen, r. D. Pettersen, and J. Hansen. *ICT Architecture Principles for the Norwegian Higher Education Sector*. September 2015. Technical Report.

[3] M. Bishop. *Computer Security: Art and Science*. 2003. Boston: Addison- Wesley.

[4] R. Covington, H. Jahangir, G. Wright, P. Silverstein, H. Dia, , and B. Rasmussen. The oracle enterprise architecture framework. *White Paper Oracle*, October 2009. http://www.oracle.com/technetwork/articles/entarch/oea-framework- 133702.pdf.

[5] D. Deighton. *Enterprise Architecture Principles*. March 2014. Technical Report, https://intranet.birmingham.ac.uk/it/documents/public/architecture/Enterprise-Architecture-Principles.pdf.

[6] M. Dowd, J. McDonald, and J. Schuh. *The art of software security assessment identifying and preventing software vulnerabilities*. 2006. Addison Wesley Professional.

[7] M. Howard. *Attack surface: Mitigate security risks by minimizing the code you expose to untrusted users*, volume 11. 2004.

[8] INFORMATION and C. TECHNOLOGY. *Enterprise Architecture Principles*. July 2015. Technical Report, http://www.usask.ca/avp-ict/stewardship/EA.

[9] G. McGraw. *Software Security: Building Security In.* 2006. Upper Saddle River, NJ: Addison-Wesley.

[10] UK Ministry of Defence. *Mod architecture framework*. December 2012. https://www.gov.uk/guidance/mod-architecture-framework.

[11] US Ministry of Defence. *The DoDAF Architecture Framework*. August 2010. http://dodcio.defense.gov/Library/DoD-Architecture-Framework/.

[12] The Executive Office of the President of the United States (EOPOTUS). *A Common Approach to Federal Enterprise Architecture*. May 2012. Technical Report.

[13] CIO Office. *WUSTL Enterprise Architecture Principles*. 2015. Technical Report, https://cio.wustl.edu/wp-content/uploads/2015/05/WUSTL-Enterprise-IT-Architecture- Principles-BYU.pdf.

[14] Queensland Government Chief Information Office. *Queensland government enterprise architecture framework 2.0 (QGEA)*. April 2009. https://www.qgcio.qld.gov.au.

[15] J. H. Saltzer and M. D. Schroeder. The protection of information in operating systems. In *in Proceedings of the IEEE*, pages 1278–1308, 1975.

[16] R. Sessions. *A Comparison of the Top Four Enterprise Architecture Methodologies*. May 2007. https://msdn.microsoft.com/en- us/library/bb466232.aspx.

[17] A. Spiessens. *Patterns of safe collaboration*. 2007. PhD thesis.

[18] P. S. Helen Sun and Sean Xu. Oracle enterprise architecture framework: Information architecture domain. *White Paper Oracle*, December 2011. http://www.oracle.com/technetwork/topics/entarch/oea-info-arch- framework-dev-process-513866.pdf.

[19] The Open Group. Togaf version 9.1, 2011. http://pubsopengroup.org/architecture/togaf9-doc/arch/.

[20] J. Viega and G. McGraw. *Building Secure Software: How to Avoid Security Problems the Right Way*. 2002. Boston: Addison-Wesley.

[21] J. A. Zachman. A framework for information systems architecture. *IBM Systems Journal*, 26(3):276, 1987. IBM Publication G321-5298.