Security-Integrated Enterprise Architecture Framework (SIEAF)

Heven Hailu
HiLCoE, Software Engineering Programme, Ethiopia
h.hailumst@gmail.com

Dereje Teferi
HiLCoE, Ethiopia
School of Information Science, Addis Ababa University, Ethiopia
dereje.teferi@gmail.com

Abstract

Sophisticated and new forms of threats to information assets makes information security one of the major concerns of enterprises. It has been argued that the integration of security in an EA (Enterprise Architecture) strengthens the effectiveness and efficiency of enterprises. Moreover, causes of system attacks are associated with the architecture of systems. Therefore, designing security oriented EA is indispensable. On the other hand, EA is an approach that can serve as a means to govern Systems of Systems (SoSs) and to study security from the perspective of all elements that influence the enterprise's system architecture. In this paper, various security and EA frameworks and their integration with each other is explored for designing SIEAF. The use of Zachman for modeling the high level of EA and Sheerwood Applied Business Security Architecture (SABSA) for security and the relation of both is described step by step. TOGAF-ADM (The Open Group Architecture Framework-Architecture Development Method) is recommended for the EA development process at mid-level following the Zachman framework guidance. At the same time, SADM (Security Architecture Development Method) should be integrated with TOGAF-ADM to address information security. Ultimately, ArchiMate, MAD (Mal-activity Diagram) and/or ISSRM-DM (Information System Security Risk Management-Domain Model) should be mapped with each other at the implementation level.

This framework comprises of the EA as well as information security risks and control mechanisms on all levels of the EA. In a nutshell, the defined framework is capable of measuring the security of the EA as a whole and provides security countermeasures based on the information flow at each layer.

Design science research method was used in this study. The design of SIEAF was based on the literature on security oriented EA frameworks as well as interviews of 17 security and EA practitioners and experts. As a result, the feedback was positive and hence the framework is considered to be both usable and useful. So the defined framework is capable of modeling all possible attack scenarios or malicious activities and their sequential presentation of operations based on the information flow of EA.

Keywords: Enterprise Architecture; EA Frameworks; Information Security Principles; Security Metrics; Security Artifact; Security Risk Management

1. Introduction

There are various literature describing enterprises consisting of numerous assets and need to be protected from being accessed by unauthorized parties, asset modification and system destruction [1]. Concerning the enterprise systems, describing the type of security that is required by a specific asset in a particular layer of the organization is crucial for securing an enterprise and its emergent behavior [2]. Designing security that assures the balance between information risks and controls is indispensable [3]. However, "based on the increasing requirements of high-quality and reliable systems, developing security-integrated EA is very challenging" [2].

EA is a comprehensive picture of enterprises that mainly aims on integration, service oriented architecture and a means of examining security [1]. More importantly, EA is an approach that manages changes, align IT with business, decrease complexity which greatly reduces costs and manages stakeholders' concerns that helps to do efficient decision making. Therefore, EA can be defined as a method that evidently demonstrates an integrated structure of information, application and IT infrastructure. On the other hand, EA investigates the

emergent features of the interaction of IT and business which is beyond the IT and business architecture or even both side by side [3]. Comparisons of various security and EA frameworks, methods, and modeling languages and their integration is explored in this paper.

There are several discussions and researches concerning the security of enterprises and defined several approaches to address the subject. One of these studies, which currently is accepted by industry standards, is the Gartner Enterprise Information Security Architecture (GEISA). The focus of this enterprise security architecture is the description of the structure by considering its compatibility with EA programs and the collaboration of both [3]. However, it has no specific methodology and modeling language for implementation and hence, modeled information security in a separate system which could lead to a potential new vulnerability. Further works in this area of study include the Zachman and SABSA frameworks. The Zachman framework is adapted to include information security [3]. But it does not specifically address security aspects. Besides, as it is not a method rather a framework, it doesn't include a specific methodology for implementing both security and EA. The SABSA framework is "the most outstanding attempt of a holistic Enterprise Information Security Architecture (EISA)" [2]. But it is adapted mainly for information security which could not abstract the entire EA including System of Systems (SoSs) and their emergent behavior equivalent to the Zachman framework. So it can be said that there have not been sufficient and comprehensive approaches that consider security integration from an early phase of EA development that include elements of any information system design which are frameworks, methods and modeling languages and information system security domain model. They depend on predefined vulnerabilities, as security is designed implicitly in the EA which could not be extracted and leads to lack of analyzability of the security features.

EA framework has an important capability in optimizing business. However, a few EA frameworks provide a comprehensive security integrated enterprise architecture framework. The aim of this paper is to develop quantifiable security metrics and its countermeasures in a graphical modeling language which comprises security and EA components and their integration with each other. This framework contains both the EA as well as the security risks and measurements on all levels of EA. It defines security baseline, gap analysis, metrics, compliance, policy, standards, guidelines, and procedures.

2. Related Work

2.1 Enterprise Architecture Frameworks

As the demand of managing complex enterprise systems has been increasing, the role of EA is taken as important to facilitate communication among the organizations' business plans and define complete frameworks [2]. The applicability of EA frameworks to abstract complex systems including its emergent behavior needs to be explored. Emergent behavior is a behavior of systems that does not depend on its individual parts, but on their relationships to one another. "All the Frameworks are applicable to a single system, but not all the frameworks are suitable for SoS" [4].

One of the most popular EA frameworks is DoDAF (Department of Defense Architecture Framework). It is a well-defined architecture and its products and their requirements are detailed and structured on four views which are the *overall view*, *operational view*, *system view* and *technical view*. However, DoDAF depends on "interface" which is not applicable to the complex systems with emergent behavior due to the fact that missing of a system, subsystem or component will make the integration impossible [4]. So DoDAF could not be applicable as a framework guide in the EA development.

MODAF (Ministry of Defense Architecture Framework) is defined to structure the integration of systems in an organization. It is the extension of DoDAF to support capability management process which added two views, strategic and acquisition [2]. But it is not suitable for the development of ultra-large systems. This is because it is product-centric and can be implemented in a single system.

QGEAF (The Queensland Government Enterprise Architecture Framework) is mainly designed to scale up the compatibility and decrease the cost of IT

infrastructure. It organizes the enterprise resources including the infrastructure [2]. Nevertheless, as it is specific to a particular system, it would not be suitable to abstract the entire EA of large systems.

TOGAF (The Open Group Architecture Framework) is described mainly to integrate IT with business. Moreover, TOGAF-ADM is being used by users of TOGAF as a guide for planning architecture. This is due to its flexibility and might be used with deliverables from other frameworks such as Zachman. ADM is a generic architecture with features of loose coupling and emergent behavior of complex systems. So TOGAF-ADM is used in the EA development process following the Zachman framework guidance.

FEAF (Federal Enterprise Architecture Framework) is defined mainly to avoid redundancy and improve resource sharing among organizations. It also includes characteristics of the Zachman framework. Though it could be suitable to model the system of systems, it cannot complement with SABSA better than Zachman as both Zachman and SABSA frameworks are alike in their structure and content.

Zachman provides a way for classification of an organization's architecture to organize "primitive" architectural information; no specific models, no methodology and no notation. The Zachman framework can be used to describe any complex entity and it is not product specific. These features of Zachman are advantageous and better than other EA frameworks for developing SoS architecture with emergent behavior since the architecture developer will have the freedom to incorporate the latest modeling techniques of emergent behavior. "The SoS architecture is a layered architecture model which allows different developers to work in parallel and ensures that changes in one layer of the protocol do not interfere with operations above and below that layer" [4].

Generally, most of the frameworks are not suitable to develop ultra large systems by including emergent behaviors [4]. Besides, all the current EA frameworks have the same aim, which is efficient use of IT to support business needs that decrease complexity and share organizational resources. However, none of these EA frameworks support an approach which measures security of an enterprise based on the existing EA products [2].

2.2 Information Security Architecture

Based on extensive literature, recent and universally accepted EISA standards are GEISA, Zachman, and SABSA. The Zachman framework is adapted to include security but does not explicitly address the security issues in EA and hence the SABSA framework is intended to fill the gaps not addressed by Zachman. Furthermore, GEISA focuses on description of structures but it does not include a specific method for implementation and it is abstract and theoretical compared to SABSA. SABSA is more practical and includes its own specific method for carrying out requirements engineering. Therefore, SABSA is the most outstanding holistic EISA that can complement with Zachman [3].

SABSA closely follows the work by Zachman, although it has been adapted to security. Moreover, there is no independent security component in FEAF. DoDAF has no any specific viewpoint of security. MODAF considers security architecture implicitly similar to DoDAF that could not be extracted and leads to lack of analyzability of the security aspects in a given organization.

In summary, it can be said that all existing EISA focus mainly on the description of structure that could comply with EA programs. This eventually led to a potential vulnerability and lack of analysability of security variables. However, none of these frameworks provides an approach that enables an enterprise to track all possible malicious activities and their sequential presentation of operations graphically based on the information flow of EA.

2.3 Security-Oriented Enterprise Architecture Frameworks

2.3.1 Enterprise Architecture Security Assessment Framework (EASAF)

According to Alshmmari, "The most efficient approach for quantifying the overall information security of a given enterprise is to measure it with respect to its EA" [2]. The approach used in [2] provides an assessment framework focused only on the middle-level (Method) abstraction that comprises the SADM and the TOGAF-ADM for security and

EA respectively. This approach needs to consider the higher level presentation (the framework) which is used to model the structured set of essential components of security and EA and their relationships; the low-level component that defines a set of rules to interpret the meaning and alignment of security and EA concepts and their relationships; and the security domain model used to understand the concepts of security criterion, vulnerability, event and risk constructs and tracks the scope of security control that avoids visualization difficulties.

This paper provides a technique to quantify possible attack developments based information flow of an enterprise via the four essential components that define the high to low-level presentation of security and EA principles. These are frameworks, methods, domain model and modelling languages.

2.3.2 Designing Secure Enterprise Architecture

Bosch [3] claims that designing secure EA approach could possibly benefit both the security and EA disciplines. These benefits include addressing the security requirements and provision of holistic view where security is adequately addressed from both security and EA perspectives.

SEAF tried to address the problem of security of an organization by assessing the as-is architecture, defines the gap and finally states the to-be security extension on the ArchiMate tool in the implementation level. The security extension in ArchiMate provides the various concepts needed to include security in the architecture specification, specifically vulnerability, threat, risk, security mechanism, and security policy. These security concepts are included in SABSA to fulfil security that is not in ArchiMate [2]. However, this kind of iterative method has a disadvantage. For instance, if the approach is applied to all the assets of a system, the EA model will blast (i.e., it will be impossible to keep track of these assets, controls and relations). Generally, the security extension on ArchiMate could bring complications of visual presentation of outcome. It is not structured and understandable especially when the method enhances after each application loop [6].

SIEAF provides security domain model at the implementation level to identify important assets of an enterprise and prioritize by aligning with EA modelling language. This avoids visualization difficulties of results as asset modelling and security tracking increases after each application round.

2.3.3 MF4EASP – The Method Framework for Developing Enterprise Architecture Security Principles

The work in [7] defined a framework for integrating information security with EA management, based on the organization's EA security principles instead of only relying on technical security mechanisms provided by the existing systems and software.

This method needs to consider detail and hierarchical EA modelling to determine the expected components from the organizational context. It is highly abstracted and lacks visualization as it doesn't consider security domain model.

So the aim of this paper is to develop a framework which comprises both EA as well as the security risks, measurements and security domain model on all levels of EA hierarchically from high to low levels.

3. The Proposed Security-Integrated Enterprise Architecture Framework (SIEAF)

The main goal of this paper is to define a framework that consists of EA principles, EA artifacts and EA metrics as well as a set of EA security related principles, security artifacts and quantifiable security metrics that measure the enterprise's security level from the perspective of business architecture and data flow at each layer. It also defines assets, risks and countermeasures in graphical model. This framework provides an organization's security experts a possibility to track the entire security change management, specifically the security of an enterprise's elements and define a rule for transforming the predefined security version of EA components. Much of the existing work has addressed security as a separate discipline when organizational architecture is developed [2]. The synergic benefits of security and EA have not been sufficiently captured [3]. Security is not addressed until the strategic design of an enterprise is

established and even business is running [6]. This way of treating enterprise's security has brought various information security problems.

The framework, SIEAF, consists of four components: *Frameworks*, *Methods*, *Domain-Model* and *Modeling Languages*. A *Framework* subdivides the structures of the viewpoints in different ranges including the relationships between these domains. This includes the SABSA and Zachman frameworks for both security and EA respectively. The second component of the framework is the *Method*, which defines a work product that describes the processes for developing the structural descriptions of the main framework step by step. This methodology comprises SADM and TOGAF-ADM for detailed explanation of both security and EA principles, artifacts and metrics. The third component is a *Modeling Language* which is defined by a consistent set of rules that interpret the meaning and alignment of security and EA concepts and their relationships. It consists of MAD and ArchiMate that describe the alignment of elements and present both the security risk treatment module and the EA, respectively. The fourth component is the *Domain-Model* which presents security requirements, security control and especially the security risk treatment element which could not be found in both modeling languages. ISSRM-DM is used to help information security developers understand the concepts of security criterion, vulnerability, event and risk constructs. Mapping between this domain model and the two modeling languages is very significant to identify and prioritize important assets and present possible attacker's action, behavior and its impact on entire assets of an enterprise.

3.1 The Framework: Corresponding Integration of Zachman and SABSA Frameworks

To achieve full-fledged and security-integrated EA framework, both Zachman and SABSA frameworks and their integration have been chosen. This is because according to Bondar *et al.* [4], "the agility is more important than technology skill. The 21st century is about agility, adjustment, adapting and creating new opportunities." Hence, both Zachman and SABSA frameworks are agile and proactive and they could outline more comprehensive structure which is the basis for the design, choice, and implementation of all subsequent EA and security controls. Furthermore, both of them are open standards. They provide comprehensive views and they complement with each other regarding their contents. They also provide the relationships between the concepts in their matrix. Except one layer, all the structures of Zachman are similar with the structures of SABSA. They are used to describe standards, for example, standards for enterprises' information systems. Each cell of the frameworks contains such a series of standards for organization's information systems [8]. Zachman matrices provide views which document the system's functional structure including key functional elements, their responsibilities, the interfaces they expose and the interactions between them and SABSA like Zachman describes the security architecture and its assurance for the enterprise based on the information flow designed by Zachman [3]. Moreover, TOGAF-ADM aligns with the first four rows of the Zachman and SABSA frameworks. For the output of each of the phases, it illustrates which views and view points in both Zachman and SABSA are applicable to the specified phase. While integrating both frameworks, iterative method is used, that is, once one of the layers of Zachman is filled in, the complementing layer in SABSA is also constructed.

Therefore, it can be concluded that the integration of SABSA and Zachman side by side to design a comprehensive approach is a perfect complement.

3.2 The Method (Processes Described to Design the Framework): Complementary Integration of TOGAF-ADM and SADM

TOGAF-ADM is flexible in that it may be used with a set of deliverables from another framework, or it may even be used in conjunction with the Zachman and SABSA frameworks [4]. TOGAF-ADM allows an organization to choose to bypass or tailor any part of the process as required. ADM is a generic method for architecture development, which is designed to deal with most system requirements. This suits well with loose coupling and emergent behavior of a SoS environment.

A widely accepted standard in EA development, especially in prescriptive and step wise processes, is

TOGAF-ADM, designed by the Open Group [9]. It is the de-facto industry standard and provides a structured approach of designing enterprise architectures. Since it is also an open standard, it is well suited for the purpose of the method. However, according to literature no single development method is the industry standard.

The TOGAF-ADM needs to include the important elements that help develop the EA method. Those are EA principles including its design, EA artifacts and EA metrics. EA artifacts are products resulting from the architecture process. Artifacts are created to "describe a system solution, or state of the enterprise" [9]. EA metrics provide understanding and knowledge whether the EA is providing a value to the business or not. Three of these elements will be complemented with the elements of SADM, that is, security principles, security-related EA principles, security-related artifacts and security metrics. According to the Open Group [9], "Within TOGAF, the role of security is acknowledged but not designed and completed". The work of the enterprise architect and security practitioner is often separated while it is really needed to be fully integrated. Hence, a method called SADM that is responsible for developing security architecture is required. It is an iterative process that enables enterprise architects to develop, assess and maintain the security assessment framework [2]. SADM defines security related EA principles because in terms of information security, EA principles that have an impact on security must be identified, assessed and maintained to achieve a more secure architecture and EA principles play a major role in deploying the organization's business strategy and once properly defined, they have a major impact on achieving the organization's vision. TOGAF-ADM and SADM are methods which are used to define the EA principles and information security principles, respectively.

3.3 The Modeling Language (rules to interpret the meaning of concepts): Integration of ArchiMate and ISSRM-DM and MAD

ArchiMate is an Open Group standard that offers an open and independent modeling language for EA. It is widely known and used in different consulting firms and supported by several tool vendors. The ArchiMate language consists of modelling elements that represent real life entities and relationships between them [6]. This model is suitable to align or map with ISSRM-DM and MAD.

ISSRM-DM protects the essential IS components. It could be used to represent asset-related, risk-related and risk treatment-related concepts. The outcome of each gives fundamental understanding about assets, vulnerabilities and threats and defines the scope of the information system security as it comprises both the business and IS assets in general [6]. Possible risks could be mitigated through implementation of controls. Search of these countermeasures is made via risk analysis. Unfortunately, after controls are defined for some particular asset, it is not visible to investigate how implementation of these countermeasures will influence the whole EA. That is why the necessity of integrating the EA and the security risk management (SRM) domain model from the initial stage remains actual and motivating. Moreover, ISSRM-DM is capable of defining the same terminology for two modeling languages, ArchiMate and MAD.

According to [6], MAD presents SRM in more detail and has smoother and continuous move between requirement engineering and design stages. Moreover, it has the biggest emphasis on the attack process and attacker behavior. In other words, it helps to add malicious activity into normal work process. So MAD is used to define the security notions for describing security structure and to graphically present ISSRM risk treatment-related concepts in a "swim lane" which would be implemented in the EA (ArchiMate modeling language). Therefore, ISSRM-DM and the two modeling languages align with each other to graphically present secure EA. The proposed SIEAF is shown in Figure 1.

The proposed framework is presented in the SABSA enterprise security architecture framework using ArchiMate Modeling language. This is because SABSA develops business-driven, threat and opportunity focused enterprise security and information assurance architectures; delivers security infrastructure solutions that traceably support critical business initiatives; and provides a future-proof

framework for information management [11]. The proposed framework is developed at contextual, conceptual, logical, functional, physical, component and operational levels.

The *Contextual Architecture layer* (business view) is the main function to identify and extract security requirements from the business environment. In this layer, EA and information security goals and objectives are presented via Zachman and SABSA, respectively. Information security goals are used to realize the protection of the EA components. Hence, based on the security requirements, the business risk model is set to realize/influence the business process model from an early stage of the EA development process. Besides, this layer addresses employee's knowledge which is presented in the ISSRM-DM as an asset that needs security.

The *Conceptual Architecture layer* (Architects view) generalizes the business concerns and considerations into policies and procedures. EA policies and Security Architecture policies produce information security architecture based on the data flow analysis policies that track the business flow among different high and low-level organizational elements.

The *Logical Architecture layer* (Designer's view) defines detailed security controls and management objectives, for example, access control and monitoring operations. This layer transforms the abstract business requirements to applicable security mechanisms and specifications. In this layer, TOGAF-ADM presents EA principles and defines EA metrics and artifacts. SADM presents and prescribes the security-related EA principles, information security principles and information security services based on the security requirements and design principles. Also SADM presents security artifacts and security metrics. Eventually the integration of information security principles and a set of security related EA principles produces a list of quantifiable security metrics that permits information security architects to swiftly and easily assess the whole security of an enterprise based on the target artifacts, i.e., tracking attacks and their behaviors which are implemented on graphical diagrams presented using MAD modeling language. The security metric is one of the monitoring parameters of information security functions that provide evidences to independent auditors that intend security program is in place in an enterprise. Moreover, it is capable of measuring the level of the entire security of the enterprise with the help of the enterprise's architectural security-related artifacts.

The *Physical Architecture layer* (Builder's view) defines information security rules, practices, procedures and information security mechanisms. Specifications described by EA business rules constrained by information system standards including business practices and procedures are defined by the EA model. In this layer security mechanisms are associated with information security functions to achieve higher maturity levels of the enterprise such as policy documentation and metrics.

The *Component Architecture layer* (Tradesman's view) shows the implementation of components and the alignment they have with each other. It is the integrated configuration and deployment of the information security standards, products and tools in complement with the EA standards, products and tools instantly side by side.

Finally, the *Operational Architecture layer* helps to do monitoring and evaluation of the functioning enterprise as well as the information security service which are performing in the EA. It is the overall security service management of the organization.

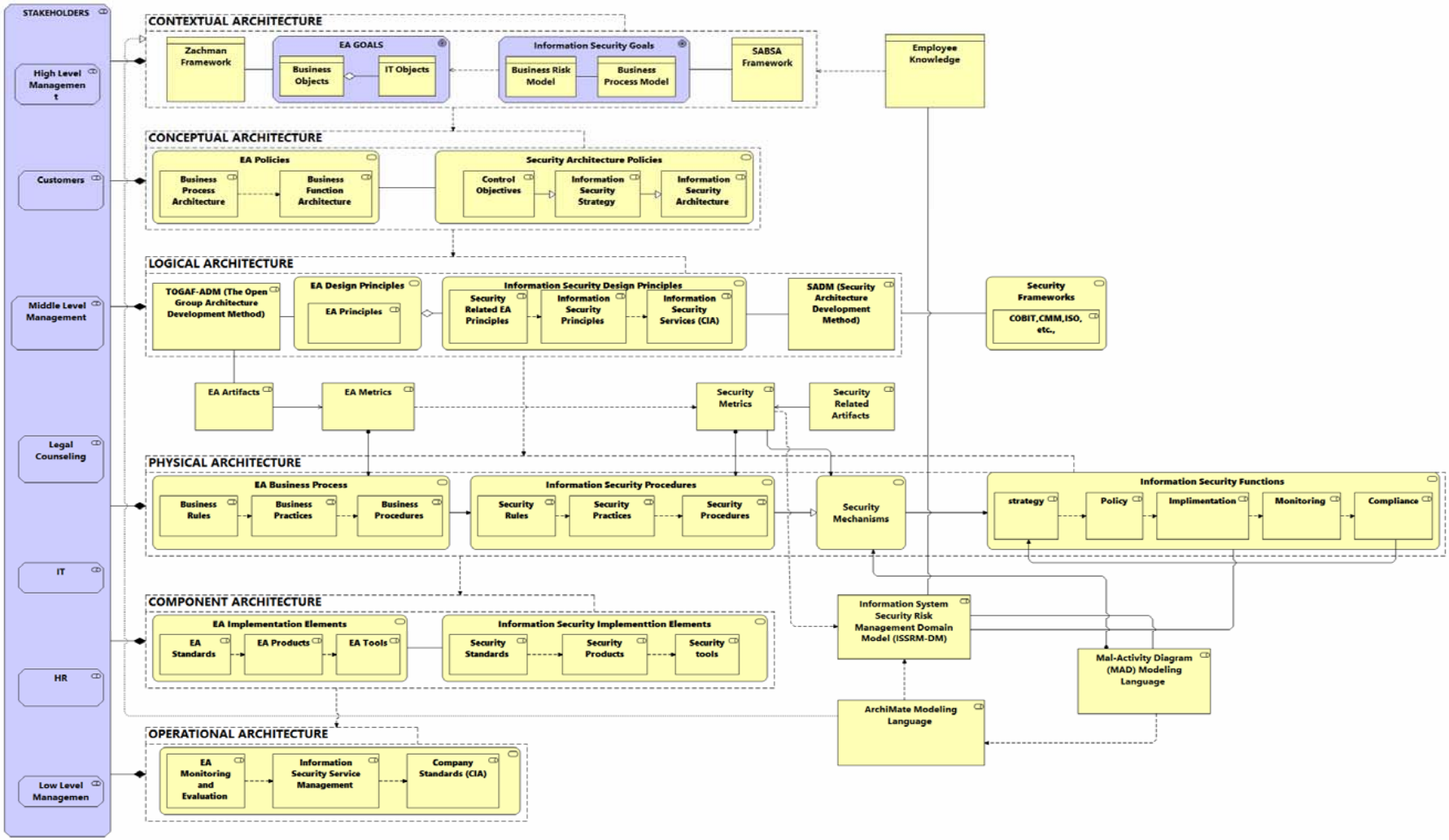

Figure 1: The Proposed Security-Integrated Enterprise Architecture Framework (SIEAF)

4. Discussion

The proposed framework is validated both internally and externally by reviewing the design process and expert interviews. Theoretical contribution of this paper has validated by research rigor. That is by the components of theoretical contribution which comprises what, how, why and the limitations of the theory by questioning who, where and when. Moreover, this framework was evaluated by relevant security and enterprise architecture experts. The evaluation is mainly on the usefulness and its degree of implementation from practical point of view. Overall the feedback was positive. However, two of the interviewees did not agree on using two modeling languages and a domain model that might result in a complex graph presentation of concepts, reducing the overview and vision. The remarks made by the experts have some implications for the suggested framework. To conclude, the approach is determined to be useful as well as usable, considering the highlighted limitations.

5. Conclusion and Future Work

The aim of the paper is to develop knowledge artifact in the form of a framework which focuses mainly on the integration of information security and EA at an initial stage of the EA development process. Information security and EA principles, which have a major effect on security, are the key ingredients of the integration.

The designed framework contributes to the currently inadequate theoretical background of knowledge, specifically to the field of EA and information security architecture and their integral relation, challenges and limitations for protection and management of business. The practicality of SIEAF should be considered relevant and valid, though the artifact still requires to be tested and validated in real environments.

In the future, studies will be carried out on application of mathematical model which quantifies the security level of each layer starting from its early EA development stage by considering EA and security design principles. The model will enable to design security sensitive enterprise assets by providing enterprise architects the ability to assess their organization automatically based on the security metrics of the enterprise.

References

[1] S. Jalaliniya and F. Fakhredin, “Enterprise Architecture and Security Architecture Development,” Unpublished Master Thesis, Lund University, 2011.

[2] B. M. Alshammari, “Enterprise Architecture Security Assessment Framework (EASAF),” Journal of Computer Sciences, 2017, 13(10), pp. 558.571.

[3] S. V. Bosch, “Designing Secure Enterprise Architectures,” Unpublished Master Thesis, Mathematics and Computer Science Enschede, the Netherlands, 2014.

[4] S. Bondar, J. C. Hsu, A. Pfouga, and J. Stjepandic, "Zachman Framework in the Agile Digital Transformation,” 2017.

[5] The Open Group, “Integrating Risk and Security within a TOGAF Enterprise Architecture,” Secur. Forum (a Forum Open Inst. Group), 2016, Available at https://publications. opengroup.org/g152.

[6] I. Tovstukha, “Management of Security Risks in the Enterprise Architecture using ArchiMate and Mal-activities,” Unpublished Master Thesis, University of Tartu, 2014.

[7] S. Larno, V. Seppänen, and J. Nurmi, “Method Framework for Developing Enterprise Architecture Security Principles,” Complex Systems Informatics and Modeling Quarterly, CSIMQ, No. 20, pp. 57–71, 2019.

[8] https://store.theartofservice.com/the-zachman-framework-toolkit.html, 2018.

[9] TOGAF Version 9.1, G116, The Open Group, 2011.

[10] Chowdhury M. J. M., Matulevičius R., Sindre G., and Karpati P., "Aligning Malactivity Diagrams and Security Risk Management for Security Requirements Definitions", 2012.

[11] V. Czaplewski CBAP, CMRP, SABSA Foundation SCF, 2017.