

Developing a Semantic Mapping between TOGAF and BSI-IT-Grundschutz

Delin Mathew¹, Simon Hacks² and Horst Lichter²

¹ RWTH Aachen University, Aachen, Germany
{delin.mathew}@rwth-aachen.de

² RWTH Aachen University, Research Group Software Construction, Aachen, German
{simon.hacks,horst.lichter}@swc.rwth-aachen.de

Abstract. Enterprise Architecture Frameworks (EAFs) are being employed vastly within various organizations in recent years. Moreover, due to the high prevalence of information technology in the enterprises, Information Security (IS) was incorporated into the EAFs. Therefore, it gradually became important for the EAFs to conform to the IS standards such as the ISO and the BSI series.

In this paper, we present a mapping of such an EAF, called The Open Group Architecture Framework (TOGAF), to an IS standard, BSI-IT-Grundschutz. Following this, we explain how a real-world Enterprise Architecture (EA) model (developed using TOGAF) of a renowned German company was mapped to BSI-IT-Grundschutz. This not only allows the various IS safeguards defined within BSI-IT-Grundschutz to be adapted to TOGAF and the EA model but more importantly, it allows the reuse of identified components of the TOGAF and the EA model, while mapping it to BSI-IT-Grundschutz using an automated tool in future.

Keywords: Enterprise architecture, TOGAF, BSI-IT-Grundschutz

1 Introduction

An Enterprise Architecture (EA) gives a conceptual outline of the structure of the enterprise, including its various processes, their inter-relationships and the principles and guidelines that determine their design and evolution [1, 2]. It also facilitates the realization of the strategic objectives of the organization [1]. An Enterprise Architecture Framework (EAF) guides in the development of an EA by generating a model or a structure which assists in the visualization of the business process and IT activities in an enterprise, based on the principles and standards set by the enterprises. This helps in optimizing the business processes by the eradication of gaps, redundancies and contradictions [3]. Since the introduction of the first EA framework by Zachman, many other EA frameworks were introduced including Federal Enterprise Architecture (FEA), or The Open Group Architecture Framework (TOGAF).

After the establishment of EA frameworks in the enterprises, information security was incorporated into some of the EA frameworks as Enterprise Information Security

Architecture (EISA), due to the increasing prevalence of information technology in enterprises and because inadequately protected information can have far-reaching repercussions on the performance of business [4, 5].

Although, many best practices like EISA are being followed to implement the security measures defined by various standards like ISO27000 series, this has been found to fall short as it is generally difficult to audit best practices and they provide no certification. Also, these best practices are not incorporated into all the EAFs (for example, TOGAF and FEA) [3]. Besides, an information security standard, like the ISO or the BSI series, is applicable to any kind of EAF and also provides a certification which proves the information security capabilities of an enterprise [6]. Therefore, it is important that EAFs conform to Information Security Management (ISM) standards to protect all kinds of information pertaining to an enterprise from all sources and to maintain the confidentiality, availability and integrity of the information [5].

Therefore, a mapping between the BSI security standard and TOGAF will not only allow the various information security safeguards defined in the BSI security standard to be adapted to TOGAF for strengthening its information security. Furthermore and more importantly, it allows reusing the identified components of TOGAF while mapping it to the BSI security standard using an automated tool in future. As a result, if someone (for example, an IT-Security officer) wishes to do the same mappings using a tool, he or she can directly employ the identified components into the tool, without having to find the components again. Consequently, we formulated our research question: *How can EAF's artefacts be efficiently reused for ISM?*

To answer this question, we developed a semantic mapping between the EAF TOGAF and the BSI Standard 100-2 [21]. Since, this standard of BSI is commonly referred to as the IT-Grundschutz methodology, we would be addressing this standard as BSI-IT-Grundschutz from here on [21]. We chose TOGAF (and not any other EAF), because it is one of the most commonly employed EAF [22]. Additionally, we chose BSI-IT-Grundschutz over the ISO standards, because the BSI standard not only covers the same content, but also describes many issues more detailed and in a didactical and informative manner [5]. Moreover, an ISO certification is always included along with the BSI certification [5].

The rest of this paper is divided into five sections. Section 2 contains a compilation of various kinds of mapping techniques that have influenced our work. After this, we depict in section 3 the applied research methodology. Section 4 explains the concept followed to achieve our solution, and the tools used, if any. We divided our solution into four parts. In the first part we created a mapping between TOGAF process and BSI-IT-Grundschutz process. After that, we applied a mapping between the components of TOGAF and BSI-IT-Grundschutz. Following this, we mapped a real-world TOGAF-based EA of a renowned German company to BSI-IT-Grundschutz. Although, this company applied TOGAF to develop its EA, ArchiMate was used to model the EA. Therefore, we first mapped the components of ArchiMate and BSI-IT-Grundschutz components and used this mapping as a meta-model for the mapping between the components of the EA model of the company (i.e., the ArchiMate model) and the BSI-IT-Grundschutz. Following this, we conducted expert interviews to

discuss the obtained mappings. The results of the discussions are outlined in section 5. The last section of this paper summarizes the findings and provides suggestions for future work.

2 Related Work

This section outlines the various published mapping techniques, which we studied in detail. We incorporated some of the techniques to realize our solution.

Zadeh et al. mapped the EA principles defined in TOGAF to the cybernetics concepts such as Viable System Model (VSM) or Viable Governance Model (VGM) to establish suitable theoretical foundation for the EA principles. After having understood the semantics and the rationale behind each TOGAF principle, a cybernetic concept that matches the rationale and semantics of the principle was chosen and mapped to it [11].

Al-Nasrawi et al. did a dual mapping between the EA frameworks such as TOGAF, FEA and Gartner Methodology with Zachman Framework and also with Software Development Life Cycle (SDLC) to select the best EA framework for achieving seamless e-government integration. This was done by mapping the frameworks to the perspectives and abstractions of the Zachman Framework and by listing the phases of SDLC and checking which frameworks support each phase within its process [12].

Holm et al. created a mapping of the meta-model of a data collection tool called NeXpose Scanner to the EA meta-model called ArchiMate for the generation of EA models using the data collected by the scanner. Specifying the means of mapping the meta-models was done manually by the researchers. After this, an existing software tool was used for the model transformation based on the specified mapping [13].

König et al. conducted a mapping of Substation Configuration Language (SCL) to ArchiMate to better enable the stakeholders to understand the Substation Automation (SA) system and its architecture. The mapping is done by identifying the SCL objects that have the relation “is a kind of” or “is a part of” to any entity of ArchiMate [14].

Alizadeh et al. conducted a mapping between the concepts of enterprise ontology (DM2 meta-model) to service concepts in the Service Oriented Architecture (SOA) for the identification of services at the enterprise level. Based on the semantic specification of the services, the concepts and aspects of services that can be mapped to the concepts of enterprise ontology were identified [15].

In [16], Santikarama and Arman developed an EAF for non-cloud to cloud migration for the companies adopting cloud computing. This EAF was developed using TOGAF, Cloud Computing Reference Model (CCRM) and Cloud Reference Migration Model (CRMM). The design of this framework involved a mapping between the TOGAF Architecture Development Method (ADM) phases with the CCRM phases and the mapping of TOGAF ADM phases with the CRMM phases.

3 Methodology

In our work, we followed the Design Science Research (DSR) Methodology defined by Peffers et al. in [8]. DSR defines a systematic approach for the creation of successful artefacts such as constructs, models, methods or instantiations [9]. The process proposed by Peffers et al. includes six steps which are: problem identification and motivation, definition of objectives, design and development, demonstration, evaluation and communication [8].

Based on this methodology, we first defined the purpose of creating a mapping between TOGAF and BSI-IT-Grundschrift by describing the major concerns that such a mapping can address (problem identification and motivation at the beginning of section 1). After this, we formalized the different objectives to be achieved and their order of execution to realize our solution (definition of objectives at the end of section 1). Later, a literature review of various research papers helped us to discover multiple approaches for conducting the mapping. After scanning through over fifteen papers that focused on mappings of various kinds, we narrowed our focus down to six papers that used the concept of semantic mapping. The methods followed by König et al. [14] and Santikarama et al. [16] in their respective works has extensively influenced the realization of our idea (justification for using these methods are provided in section 4.1-4.3 of this paper). We demonstrated our idea by applying it to derive the mappings between TOGAF and BSI-IT-Grundschrift and later in deriving the mappings between the EA model and BSI-IT-Grundschrift (design and development in section 4.1-4.3 and demonstration in section 4.4). We discussed our findings by conducting expert interviews. Later, we used the results and feedback obtained from the expert interviews to improve our results (feedback loop from discussion with experts to design and development in section 5). The communication is done by publishing the obtained results in this paper. Furthermore, all our results can be accessed via <https://git.rwth-aachen.de/EARTh/Mapping>.

4 Concept and Realization

Within this section, we facilitate the design and development step of Peffers et al. [8]. First, we map the processes of TOGAF to the processes of BSI-IT-Grundschrift. Second, we map the components of TOGAF to those of BSI-IT-Grundschrift. Third, we map the ArchiMate's components with the BSI-IT-Grundschrift components. Last, we demonstrate our mappings by applying it to a company's EA model according to the fourth step of DSR.

4.1 Mapping between TOGAF Process and BSI-IT-Grundschrift Process

The TOGAF process refers to the TOGAF ADM [2]. Similarly, the BSI-IT-Grundschrift also includes a security process which helps in the development of an Information Security Management System (ISMS) [21].

The idea was to first visualize each process from a higher level of abstraction. After understanding each phase of both processes, we sketched out a common process model for both processes, which is depicted in fig. 1 (center). This common process model was obtained based on quite a few similarities shared by the processes, out of which the first one being the iterative nature of the two processes. Fig. 1 shows that after the first phase of each process, which is the initiation phase (“preliminary phase” in case of TOGAF and “initiation of security process” phase in BSI-IT Grundschutz), the rest of the phases are iterative. Also, it can be observed that both processes have a similar structure. Each of the processes starts off with an initiation phase where the planning and defining of the scope takes place. This is followed by the creation phase where the creation of the main parts of the target state takes place. After this, the actual realization and implementation of the goal or the target state takes place. Finally, the already implemented target state gets improved [2, 21]. The technique applied here is inspired from the mapping technique mentioned in [16] as it also focuses on creating a mapping between different processes. Additionally, we also developed a meta-model for our mapping.

Based on the meta-model, the initial two phases of TOGAF, which are the Preliminary phase and the Architecture Vision, were mapped to the first step of the BSI-IT-Grundschutz process, which is the Initiation of Security Process (this corresponds to the initiation phase of the meta-model). The common activities that led to this mapping included: defining of scope, identifying organizational units, forming of teams, identifying stakeholders, defining resources, identifying gaps and getting management approval [2, 21].

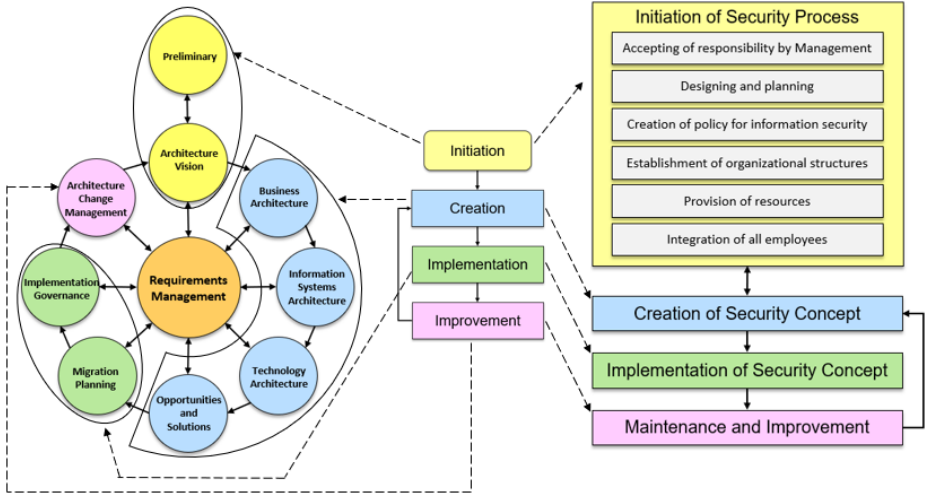


Figure 1: Mapping of the TOGAF process (left) to the BSI-IT-Grundschutz process (right) based on the derived common process model (center)

The following four phases of TOGAF were mapped to the second step of the BSI-IT-Grundschutz process, which is the Creation of the Security Concept (this corresponds to the creation phase of the common process model). The common

activities in this case included: creating the main parts (in the case of TOGAF, the enterprise architecture and in the case of BSI-IT-Grundschutz, the security concept), obtaining stakeholder reviews, resolving gaps, mitigating risks and documentation of building blocks in case of TOGAF and in the case of BSI-IT-Grundschutz, its various components [2, 21].

The Migration Planning and Implementation Governance phases of TOGAF were mapped to the Implementation of Security Concept phase of BSI-IT-Grundschutz process (this corresponds to the implementation phase of the common process model). The common activities that led to this mapping included: developing the implementation plan, conducting cost-benefit analysis, checking availability of resources and conducting compliance reviews [2, 21].

Finally, the Architecture Change Management phase was mapped to the last step of BSI-IT-Grundschutz process which is Maintenance and Improvement (this corresponds to the improvement phase of the common process model). The common activities in this case included- conducting management reviews, documenting of results, checking the business value and maintenance [2, 21].

4.2 Mapping between TOGAF Components and BSI-IT-Grundschutz Components

The mapping between TOGAF and BSI-IT-Grundschutz components was conducted manually as there did not exist a tool for this specific mapping. The approach was to scan the entire TOGAF document and identify all the components and map them to the appropriate BSI-IT-Grundschutz components. This was performed by analyzing the BSI-IT-Grundschutz catalogues [4] and determining the components that were equivalent or related to the TOGAF components.

Once a BSI-IT-Grundschutz component is identified and mapped to a TOGAF component, the corresponding security safeguards associated with the BSI-IT-Grundschutz component are also assigned to the TOGAF component. Note that, in our work, the TOGAF components were first identified and mapped to the BSI-IT-Grundschutz modules and not the other way around. This was motivated by the fact that most of the elements in BSI-IT-Grundschutz are a general representation of the components in TOGAF.

Since these are two completely different processes focusing on different goals, a specific mapping between the components of TOGAF and BSI-IT-Grundschutz was a rare occurrence. Therefore, we chose to follow a mapping technique similar to the one employed by König et al. in [14]. When a direct mapping was not obtained, the TOGAF component was mapped to those BSI-IT-Grundschutz components which had the relation “is a kind of” or “is a part of” to the TOGAF component, as in [14]. After conducting the mapping task, a total of 873 mappings were obtained. These mappings can be divided into two types: 1:1 and 1:N. In a 1:N mapping, one component in TOGAF was mapped to multiple components in BSI-IT-Grundschutz, whereas, for a 1:1 mapping, only discrete components from both the processes were mapped together. A 1:1 mapping becomes a specific mapping when there is a perfect

match between discrete components from each process. Consequently, all the 1:N mappings are non-specific.

Some of the mappings that were obtained are:

- Databases ↔ Databases: This is a 1:1 mapping and is also a specific mapping. The component on the left belongs to TOGAF and the component on the right belongs to BSI-IT-Grundschrift.
- Data Server ↔ General Server: Here, the TOGAF component “Data Server” was mapped to “General Server”. This is another example of a 1:1 mapping. But, this is not a specific mapping. Therefore, this was mapped to the closest possible component in BSI-IT- Grundschrift which is “General server” [4]. Therefore, the relationship here is: Data Server “is a part of” General Server.
- Telephone ↔ Telecommunications system, Mobile telephones: This is a 1:N mapping. “Telephone” was mapped to “Telecommunications system” because Telephone “is a part of” Telecommunications system and “Telephone” was also mapped to “Mobile telephones” as Mobile telephones “is a kind of” Telephone.

4.3 Mapping between ArchiMate Elements and BSI-IT-Grundschrift Components

The concept followed for the mapping between ArchiMate and BSI-IT-Grundschrift components was very similar to the one used in the previous section. Here as well, a manual mapping among related components was carried out. For the mapping, we considered the components of BSI-IT-Grundschrift and mapped them to suitable ArchiMate elements, obtained from the various layers of the ArchiMate framework [7]. It should be noted that, unlike in the previous case (where the TOGAF components were mapped to the BSI-IT-Grundschrift modules), the BSI-IT-Grundschrift modules were mapped to the ArchiMate elements and not the other way around. This was motivated by the fact that most of the elements in ArchiMate are a general representation of the components in BSI-IT-Grundschrift.

Like the previous case, these are also two completely different processes trying to achieve different things. So, a specific mapping between the components of BSI-IT-Grundschrift and ArchiMate was not feasible. Therefore, we once again employed the mapping technique inspired by König et al. in [14]. After conducting the mapping task, a total of 80 mappings were obtained. The mappings were divided into two types: 1:1 and 1:N. Some of the mappings that were obtained are:

- Server Room ↔ Facility: The component on the left belongs to BSI-IT-Grundschrift and the component on the right belongs to ArchiMate. This is a 1:1 mapping and it is not a specific mapping. There is no component in ArchiMate that can be directly mapped to “Server Room” [4] from BSI-IT-Grundschrift. Therefore, we mapped “Server Room” to the closest possible element in ArchiMate which is “Facility” [7]. The resultant relationship is: Server room “is a kind of” Facility.
- Security Management ↔ Business Service, Technology Function: This is a 1:N mapping. Here, the BSI-IT-Grundschrift component “Security Management” [4]

was mapped to two components in ArchiMate “Business Service” and “Technology Function” [7]. Here the relationship is Security Management “is a kind of” Business Service and it is also “a kind of” Technology Function.

4.4 Mapping between the Components of Company’s EA Model and BSI-IT-Grundschatz Components

Case Environment: The Company considered in our work is a leading insurance provider in Germany. It operates in over 30 countries and has over 40,000 employees. It has several subsidiaries, including an internal IT service provider, which we considered for our work. The IT service provider has over 1,400 employees and provides technological solutions for the entire organization. It used the TOGAF framework to develop its EA and a tool called Archi¹, an ArchiMate tool, to develop of EA model.

Using the results of the mapping between ArchiMate and BSI-IT-Grundschatz components as a meta-model, a mapping between the components of the company’s EA model and BSI-IT-Grundschatz components was developed. The first step was to analyze the elements in the different ArchiMate layers (business layer, application layer, technology layer and so on) of the EA model and the relationship between the elements of the same or different layers. The second step was to map these elements to the BSI-IT-Grundschatz components. This was done by using a tool called Verinice² that facilitates the creation and management of an ISMS using BSI-IT-Grundschatz [17]. The BSI model in Verinice consists of different groups into which the ArchiMate elements should be grouped under, prior to the mapping to the BSI-IT-Grundschatz components. The Verinice tool not only allows the mapping of the ArchiMate elements to the BSI-IT-Grundschatz components, but also helps in modeling the relationships between the elements.

Modeling Elements in Verinice. After analyzing the ArchiMate elements in the EA model, it was found that some of the elements such as technology functions, technology services, business functions, business processes or products could not be included under the groups in the BSI model of Verinice, because the groups can only include the elements related to applications, IT-systems, network connections, rooms and staff. On the other hand, elements such as devices, nodes, system software, application collaboration, business actors could be included under the groups in the BSI model.

But the fact that some elements could not be included made it complicated to model relationships between elements in Verinice. For example, consider a web application which has a “used by” relationship with a technology service called content service which has a “realization” relationship with a data server (see fig. 2). As mentioned before, the technology service cannot be included in the different groups of Verinice, whereas, the web application and the data server can be included. Hence, it was not possible to model the relationships between the web application and

¹ <https://archimatetool.com>

² <https://verinice.com>

the content service, and between content service and data server in Verinice. Consequently, a relationship between web application and data server needs to be modeled. In such cases, a relationship needs to be derived between the two elements that do not have a direct relationship.

A workaround to this was found in the paper by Buuren et al. [18]. In their work, they first assigned a weight to every relationship type in ArchiMate, based on the semantics and understanding of the relations. They defined a composition operator which derives a relationship based on the weight of the existing relationships. And during the derivation, the relation type with the most minimum weight is derived. So, in this case between “used by” and “realization”, “used by” relation had lesser weight when compared to “realization” according to [18]. Therefore, a “used by” relation was derived between the web application and data server. Based on this principle, we were able to model the relationships between EA elements in Verinice even though many elements of the EA model could not be included in the Verinice tool.

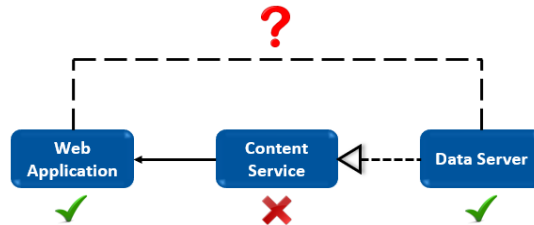


Figure 2: Multi-Step Relation

Modeling Relationships in Verinice. It was observed that not every element included in Verinice could be related to every other element. For example, an element under the group clients in Verinice can only have a relationship with the elements included under the group’s applications, staff and room. It cannot be related to elements in the other groups in Verinice such as buildings, clients, network components, PBX components, servers and network connections.

The relationship types in the ArchiMate such as composition, aggregation, association and so on does not exist in the Verinice tool. Verinice has its own set of relation types such as depends on, responsible for or necessary for. For example, consider an element under the group staff that has an association relationship with an element in the applications group. The relationship types available in Verinice for a relation between these two elements are “accountable for”, “consulted for”, “informed about” and “responsible for”.

Mapping ArchiMate Elements to BSI-IT-Grundschatz Elements. After having assigned the EA elements in the various groups of the BSI model in Verinice and having modeled the relationship between the elements, the next step was to map these elements to the BSI-IT-Grundschatz components. This can be done by dragging and dropping the appropriate BSI-IT-Grundschatz components under the suitable EA elements. Along with the BSI-IT-Grundschatz components, the security safeguards corresponding to those components will also be assigned to the elements.

Advantages and Disadvantages of Verinice. We summarize this section with the various advantages and disadvantages of Verinice. On one hand, Verinice is a tool

that facilitates the creation of an ISMS based on BSI-IT-Grundschutz, it allows easy mapping to the BSI-IT-Grundschutz components using drag and drop method, supports easy implementation of safeguards, allows relationship modeling, provides protection requirements, and performs basic security check and risk analysis. On the other hand, not all elements can be modelled in Verinice; there exists difficulty in modeling relationships, not every element can be related to every other element and ArchiMate relationship types cannot be modelled in Verinice.

5 Discussion

To discuss our obtained results, we conducted expert interviews. For the first discussion, we required someone with a good insight about BSI-IT-Grundschutz and for the second discussion we required an internal employee of the company who is familiar with the EA model. According to [10], the main purpose of expert interviews is to discuss and evaluate something that requires specific subject knowledge and in some cases insider knowledge on the related topics.

5.1 Discussion of the TOGAF and BSI-IT-Grundschutz Components Mapping

Since the mappings obtained were very high in number, a small sample of mappings was considered for the discussion. The method of stratified random sampling [19] was used to obtain a finite list of mappings. This was done by removing the duplicate mappings and dividing the entire group of mappings into homogeneous sub-groups called strata. While the elements within a stratum are mutually inclusive (homogeneous), each stratum should be mutually exclusive to each other. Then a simple random sampling is applied to each stratum where an element is randomly chosen from each stratum to generate the final sample.

The discussion was conducted by two experts who were well-versed with BSI-IT-Grundschutz. The goal of our work and the approach used to achieve the goal were briefed to each discussant. Thereupon, each mapping, along with its justification, was presented to them. The discussants were asked to rate each mapping on a 5-point Likert scale [20]. Along with the rating for each mapping, the feedback obtained for the mappings were duly noted. Both the discussants agreed with 90% of the mappings in the list provided to them and they found the mappings to be mostly accurate. After carefully assessing the feedback given by discussants, the necessary changes were made to the mappings.

5.2 Discussion of the Mapping between the Components of Company's EA Model and BSI-IT-Grundschutz Components

We discussed the proposed mapping with an employee of the company who was closely associated with the development of the company's EA. The entire process involved in the mapping, along with an example was illustrated to the discussant.

Unlike the previous discussion, instead of asking the discussant to rate the mapping, the discussant's feedback (both positive and negative) was collected.

In the discussant's opinion, the mapping will be particularly useful for data objects, system software, applications that use databases and application services. She felt that the mapping was very useful and would definitely benefit the company if done systematically and preferably by an internal person who has the necessary business knowledge. On a negative note, she felt that, even though the elements such as data objects and application services could be mapped to certain BSI-IT-Grundschatz components, it is a setback that these elements cannot be modeled in Verinice. Also, in her opinion, it would make the searching of the modules easier if the BSI-IT-Grundschatz components were categorized in Verinice.

6 Conclusion

The main aim of our work was to develop a mapping between TOGAF and BSI-IT-Grundschatz based on semantics. To better understand both processes and their similarities, a process to process mapping between TOGAF and BSI-IT-Grundschatz was done beforehand. For the complete realization of our solution, a real-world example of an EA model of a German company, developed using TOGAF, was considered and mapped to BSI-IT-Grundschatz using the Verinice tool. This mapping does not only allow organizations to strengthen their information security of TOGAF, ArchiMate and the EA model, but also allows reusing the identified components of TOGAF, ArchiMate and the EA model while conducting such a mapping using an automated tool in the future.

Although we were able to identify a large number of components for the mapping, the shortcomings of manual mapping such as accidental exclusion of components and creation of the mappings only based on the subjective understanding are undeniable.

We propose the following improvements to be implemented in the future. The first one is to automate the mapping using the identified components of TOGAF, ArchiMate and the EA model in a tool. This will provide accurate and faster results because as opposed to manual mapping, human errors could be eliminated. The second improvement would be to customize the Verinice tool to accommodate the mapping between BSI-IT-Grundschatz and the EA model in a more native way by allowing all the ArchiMate elements and relationships to be modelled in Verinice.

References

1. Proper, E., and Greefhorst, D.: The Roles of Principles in Enterprise Architecture. In: Trends in Enterprise Architecture Research. 5th International Workshop, TEAR, pp. 57–70. Springer, Berlin, Heidelberg, (2010)
2. TOGAF®9.1, <http://pubs.opengroup.org/architecture/togaf9-doc/arch/> (Accessed on 05/22/2017)

3. Oda, S.M., Fu, H., and Zhu, Y.: Enterprise information security architecture a review of frameworks, methodology, and case studies. In: Computer Science and Information Technology, 2nd IEEE International Conference, pp. 333–337. IEEE, ICCSIT (2009)
4. IT-Grundschutz-Catalogues. Standard. Federal Office for Information Security, Bonn, Germany (2013)
5. BSI Standard 100-1: Information Security Management Systems (ISMS). Standard. Bundesamt für Sicherheit in der Informationstechnik (BSI), Bonn, Germany (2008)
6. Granneman, J.: IT security frameworks and standards: Choosing the right one. Article. (2013)
7. ArchiMate 3.0 Specification. Standard. The Open Group, Berkshire, United Kingdom, (2016)
8. Peffers, K., Tuunanen, T., Rothenberger, M.A., and Chatterjee, S.: A Design Science Research Methodology for Information Systems Research. Journal of Management Information Systems, Routledge (2007)
9. Hevner, A.R., March, S.T., and Park, J.: Design Research in Information Systems Research. pp. 75-105 MIS Quarterly, 28, 1 (2004)
10. Bogner, A., Littig, B. And Menz, W.: Interviewing Experts (Research Method Series). Palgrave Macmillan Limited, England (2009)
11. Zadeh, M. E., Millar, G. and Lewis, E.: Mapping the enterprise architecture principles in TOGAF to the cybernetic concepts—An exploratory study. In: System Science (HICSS), 2012 45th Hawaii International Conference, pp. 4270–4276. IEEE. (2012)
12. Al-Nasrawi, S. and Ibrahim, M.: An enterprise architecture mapping approach for realizing e-government. In: Communications and Information Technology (ICCIT), 2013 Third International Conference, pp. 17–21. IEEE. (2013)
13. Holm, H. and Buschle, M.: Automatic data collection for enterprise architecture models. In: Software & Systems Modeling, pp. 825–841. 13.2 (2014)
14. König, J., Zhu, K. and Nordstorm, L.: Mapping the substation configuration language of iec 61850 to archimate. In: Enterprise Distributed Object Computing Conference Workshops (EDOCW), 2010 14th IEEE International, pp. 60–68. IEEE. (2010)
15. Alizadeh, K., Seyyedi, M. A. and Mohsenzadeh, M.: Mapping service concept and enterprise ontology in service identification. In: Networked Computing (INC), 2011 The 7th International Conference, pp. 22–27. IEEE. (2011)
16. Santikarama, I. and Arman, A. A.: Designing enterprise architecture framework for non-cloud to cloud migration using TOGAF, CCRM, and CRMM. In: ICT For Smart Society (ICISS), 2016 International Conference, pp. 32–37. IEEE. (2016)
17. verinice. / Produkt, <https://verinice.com/produkt/> (Accessed on 05/22/2017)
18. Buuren, R. v., Jonkers, H., Iacob, M. and Strating, P.: Composition of relations in enterprise architecture models. In: International Conference on Graph Transformation, pp. 39–53. Springer. (2004)
19. Neyman, J.: On the two different aspects of the representative method: the method of stratified sampling and the method of purposive selection. In: Journal of the Royal Statistical Society 97.4, pp. 558–625. (1934)
20. Dawes, J.G.: Do data characteristics change according to the number of scale points used? An experiment using 5 point, 7 point and 10 point scales. In: (2012)
21. BSI Standard 100-2: IT-Grundschutz Methodology. Standard. Bundesamt für Sicherheit in der Informationstechnik (BSI), Bonn, Germany (2008)
22. U. Franke et al.: EAF2 - A Framework for Categorizing Enterprise Architecture Frameworks. In 10th ACIS International Conference on Software Engineering, Artificial Intelligences, Networking and Parallel/Distributed Computing, pp. 327–332. (2009)