An Integrated Conceptual Model for Information System Security Risk Management and Enterprise Architecture Management Based on TOGAF

Nicolas Mayer, Jocelyn Aubert, Eric Grandry, Christophe Feltus

An Integrated Conceptual Model for Information System Security Risk Management and Enterprise Architecture Management based on TOGAF

Nicolas Mayer[1], Jocelyn Aubert[1], Eric Grandry[1], Christophe Feltus[1]

[1] Luxembourg Institute of Science and Technology, 5 Avenue des Hauts-Fourneaux, L-4362 Esch-sur-Alzette, Luxembourg
{nicolas.mayer, jocelyn.aubert, eric.grandry, christophe.feltus}@list.lu

Abstract. Risk management is today a major steering tool for any organization wanting to deal with Information System (IS) security. However, IS Security Risk Management (ISSRM) remains difficult to establish and maintain, mainly in a context of multi-regulations with complex and inter-connected IS. We claim that a connection with Enterprise Architecture Management (EAM) contributes to deal with these issues. According to our research agenda, a first step towards a better integration of both domains is to define an EAM-ISSRM conceptual integrated model. To build such a model, we will improve the ISSRM domain model, a conceptual model depicting the domain of ISSRM, with the concepts of EAM. The contribution of this paper is focused on the improvement of the ISSRM domain model with the concepts of TOGAF, a well-known EAM standard.

Keywords: Information Security, Risk Management, Enterprise Architecture, TOGAF, Compliance

1 Introduction

Nowadays, Information System (IS) security and Risk Management (RM) are required for every organization that wishes to survive in this networked world. Whether for purely compliance purposes, business development opportunities, or even governance improvement, organizations tend to implement a security strategy based on an IS Security RM (ISSRM) approach. However, organizations have to deal with pressures that increase the complexity of managing security risks: regulatory pressure involving ISSRM requirements [1–3], increasing number of threats and complexity of current IS [6, 7], lack of efficiency in the process followed [1], or difficulty to have a clear and manageable documentation of ISSRM activities [1]. Due to this complexity, new solutions are required to address security risks. Classical ISSRM methods [1, 2] are indeed not suitable to deal with the complexity of organizations and associated risks, in a context of compliance and governance.

Enterprise Architecture Management (EAM) has shown to be a valuable and engaging instrument to face enterprise complexity and the necessary enterprise transformation [3, 4]. EAM offers means to govern complex enterprises, such as, for example, an explicit representation of the enterprise facets, a sound and informed decisional framework, a continuous alignment between business and IT, and so forth [5]. By integrating EAM with ISSRM, we aim to be able to deal with the preceding listed issues related to the complexity of organizations and associated risks.

In earlier work, we have integrated the concepts of existing ISSRM standards and methods into a domain model, that we called the ISSRM domain model [6]. The goal of our research is to improve this model by extending it to a framework (modelling language, method, and tool) that incorporates results from EAM research [7] and that can be used in practice. A first step is to define an integrated EAM-ISSRM conceptual model which will be called the "EAM-ISSRM integrated model". This paper describes part of this work and its contribution is focused on analysing if and how the concepts that are part of TOGAF, a well-known standard in the domain of EAM published by The Open Group [8], can be used to improve the ISSRM domain model. Note that we do not propose a modelling language, although this task is part of our next objectives, but we define an underlying conceptual model for such a language. This model will be a key artefact towards the definition of a dedicated modelling language and of the associated ISSRM method.

In the following section, the background of our work is described: it introduces the ISSRM domain model and the TOGAF standard. Section 3 presents the conceptual alignment between the concepts of TOGAF and those of the ISSRM domain model, and then explains the key conclusions. An integrated EAM-ISSRM conceptual model based on TOGAF is proposed in Section 4. Section 5 is a comparison with related work. Finally, conclusions and future work are presented in Section 6.

2 Background

2.1 The ISSRM Domain Model

In our preceding work, the concepts of ISSRM have been represented as a domain model, i.e. a conceptual model depicting the studied domain [6]. The ISSRM domain model was designed from related literature [1]: risk management standards, security-related standards, security risk management standards and methods, and security requirements engineering frameworks. The ISSRM domain model is composed of 3 groups of concepts: *Asset-related concepts*, *Risk-related concepts*, and *Risk treatment-related concepts*. Each of the concepts of the model has been defined and linked one to the other, as represented in Fig. 1.

Asset-related concepts (light grey boxes) describe assets and the criteria which guarantee asset security. An asset is anything that has value to the organization and is necessary for achieving its objectives. A business asset describes information, processes, capabilities, and skills inherent to the business and core mission of the organization, having value for it. An IS asset is a component of the IS supporting

business assets like a database where information is stored. In our context, and as described in the ISSRM literature [1], an IS is a composition of hardware, software, network, people and facilities. A security criterion characterises a property or constraint on business assets describing their security needs. The most common security criteria are confidentiality, integrity and availability. A security objective is the application of a security criterion on a business asset (e.g. the confidentiality of personal information).

Risk-related concepts (white boxes) present how the risk itself is defined. A risk is the combination of an event with a negative impact harming the assets. A negative impact describes the potential negative consequence of an event that may harm assets of a system or organization, when an event causing this impact occurs. An event is the combination of a threat and one or more vulnerabilities. A vulnerability describes a characteristic of an IS asset or group of IS assets that can constitute a weakness or a flaw that can be exploited by a threat. A threat characterises a potential attack or incident, which targets one or more IS assets and may lead to the assets being harmed. A threat consists of a threat agent and an attack method. A threat agent is an agent that can potentially cause harm to IS assets. An attack method is a standard means by which a threat agent carries out a threat.

Risk treatment-related concepts (dark grey boxes) describe what decisions, requirements and controls should be defined and implemented in order to mitigate possible risks. A risk treatment is an intentional decision to treat identified risks. A security requirement is a desired property of an IS that contributes to a risk treatment. Controls (countermeasures or safeguards) are a designed means to improve security, specified by a security requirement, and implemented to comply with it.

2.2 TOGAF

TOGAF is a framework — a detailed method and a set of supporting tools — for developing an enterprise architecture [8]. It is a standard established and maintained by The Open Group, an industry consortium focused on IT standards. A key aspect of TOGAF is the TOGAF Architecture Development Method (ADM), a tested and repeatable process for developing architectures. The ADM includes establishing an architecture framework, developing architecture content, transitioning, and governing the realization of architectures. The TOGAF Architecture Content Framework (ACF) provides a structural model for architectural content, developed all along the different steps of the ADM, which allows major work products to be consistently defined, structured, and presented. The TOGAF ACF is structured according to its Content Metamodel. This metamodel is a single view that encompasses all four of the TOGAF architecture domains (Business, Data, Application; and Technology Architecture), and that defines a set of entities that allow architectural concepts to be captured, stored, filtered, queried, and represented in a way that supports consistency, completeness, and traceability. The TOGAF Content Metamodel and its associated glossary are of particular interest for the analysis performed in this paper. More information about TOGAF can be found in the TOGAF 9.1 reference book [8].

3 Conceptual Alignment Between Concepts of TOGAF and Concepts of the ISSRM Domain Model

The conceptual alignment consists of identifying the semantic correspondence between concepts of TOGAF and concepts of the ISSRM domain model. This task has been performed by a focus group composed of five people. Three of them are ISSRM experts and two of them EAM experts. All of the members of the focus group are researchers having a good theoretical knowledge of ISSRM and/or EAM. Moreover, two ISSRM experts are also experienced ISSRM practitioners (in total during the 10 last years, they have performed more than 20 real-world applications of ISSRM in organizations, going from SMEs to European institutions). The EAM experts are practitioners in the discipline, regularly facing real challenges from enterprises, and one of them demonstrate proven experience in the application of the TOGAF framework: rolling out the ADM in large companies, setting up and customizing TOGAF repositories corporate-wide and in the scope of projects. Alignment decisions were taken only once a consensus has been found among the members of this focus group.

3.1 Alignment Approach

The approach followed is inspired by Zivkovic et al. [9]. Each relation between concepts is classified according to the following semantic mapping subtypes:

- ***Equivalence***: *concept A* is semantically equivalent to *concept B*;
- ***Generalisation***: *concept A* is a generalisation of *concept B*, i.e. *concept B* is a specific class of *concept A*;
- ***Specialisation***: *concept A* is a specialisation of *concept B*, i.e. *concept B* is a generic class of *concept A*;
- ***Aggregation***: *concept A* is composed of *concept B*, i.e. *concept B* is a part of *concept A*;
- ***Composition***: *concept A* is composed of *concept B* (with strong ownership), i.e. *concept B* is a part of *concept A* and does only exist as part of *concept A*;
- ***Association***: *concept A* is linked to *concept B*.

The output of this step is a table, highlighting the relations between the concepts of TOGAF and those of the ISSRM domain model. Such a table is presented in a technical report [10] which aims to perform similar work with other EAM references including ArchiMate, DoDAF and IAF.

3.2 Alignment Key Conclusions

Based on the definitions of the TOGAF Content Metamodel [8], and the definitions of the concepts of the ISSRM domain [1, 6], the conceptual alignment aims at finding the structural and semantic correspondences of the concepts defined in TOGAF with

those of the ISSRM domain model. In other words, the alignment highlights the capabilities of the TOGAF approach to represent ISSRM concepts.

A detailed analysis of the results of the mapping is given next.

- Most of the core concepts of Business Architecture in TOGAF are specific kinds of Business Assets. *Capability* is also considered as a Business Asset, although it is not part of Business Architecture concepts.
- All of the TOGAF concepts of the Data, Application, and Technology Architectures are specialisations of the concept of IS asset. More specifically, they are representing IT assets, i.e. IS assets of hardware, software or network kind. The only exception is *Technology Component* which is an abstract entity, as well as the concept of *Business Service,* which is a specialisation of Business asset.
- Data, Application, and Technology Architectures are adapted to represent an IT system, but are lacking people and facilities class of IS assets, necessary to define an IS in an information security context. However, they can be represented with the help of the following concepts of the Business Architecture: *Organization Unit*, *Actor* and *Location*.
- *Event* has no mapping with any ISSRM concept. It is defined as an organizational state change that triggers a *Process*, and has thus no correspondence with concepts of the ISSRM domain model. The ISSRM domain model aims indeed at identifying structural concepts at stake, and not at handling behavioural and methodological aspects of ISSRM.
- *Gap* and *Work Package* have also no mapping with any ISSRM concept. They are related to the project management aspects of architecture design and have thus no correspondence with concepts of the ISSRM domain model.
- *Driver* is a generalisation of the Security criterion concept. In our context, we have one main concern that is IS security, leading to drivers that are ISSRM security criteria (i.e., confidentiality, integrity, availability, etc.). Regarding our scope, the conditions that motivate the organization to define its (security) goals are related to the need of confidentiality, integrity or availability of information processed in the IS. In the same vain, the concepts of *Goal* and *Objectives* are a generalization of Security objective.
- *Measure* is considered as a generalisation of Risk, because a risk is a specific kind of measure. A risk is indeed an indicator or factor that can be tracked to determine success or alignment with *Objectives* and *Goals* (i.e. confidentiality, integrity and/or availability of Business Assets).
- *Requirement* is a generalization of Security requirement.
- The concepts of *Principle* (e.g., standard to be followed, regulation, etc.), *Constraint* (e.g., customer data is not harmonized within the organization) and *Assumption* (e.g., the application to be used shall be security certified) are associated with the concept of Asset, as well as *Organization Unit* and *Role*, because the latter can also be used to represent stakeholders (e.g. regulation organization, customers, shareholders, etc.). All of these concepts are indeed used in TOGAF to represent aspects considered as part of the environment of the assets and identified during the context establishment step of the ISSRM process [2].

Concepts currently composing the ISSRM domain model are the set of concepts used during risk assessment and risk treatment steps.

To summarize, we can draw two main conclusions from the alignment. First, although the mapping is complex, TOGAF brings a more fine grained representation of (business and IS) assets than the ISSRM domain model. Second, TOGAF considers the concepts that are part of the environment of the assets. This is not the case of the ISSRM domain model.

4 EAM-ISSRM Integrated Model Proposal Based on TOGAF

The preceding conceptual alignment between TOGAF and the ISSRM domain model, and more specifically the key conclusions coming from this alignment, have highlighted that a set of concepts of TOGAF, when used in an ISSRM context, are specialisations of ISSRM concepts:

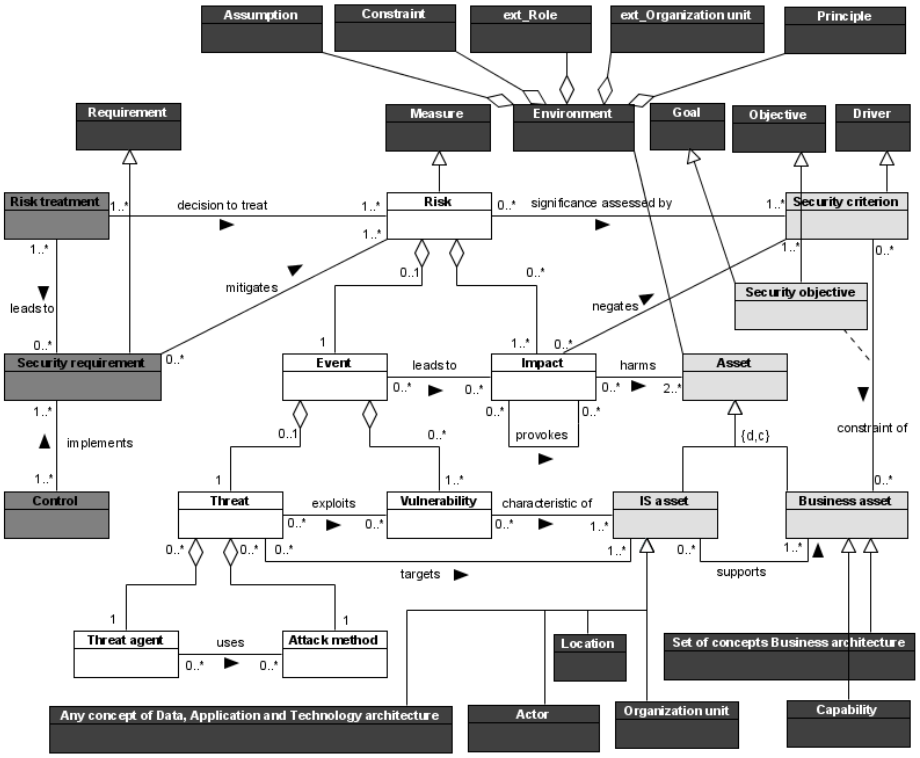

Fig. 1. EAM-ISSRM integrated model based on TOGAF

- The concepts of the Business architecture are specialisation of Business asset, except *Location*, *Actor* and *Organization unit* that are specialisation of IS asset. *Capability* is also a specialisation of Business asset.

- The concepts of the Data, Application and Technology architecture are specialisation of IS assets except *Technology Component* that is an abstract entity.

Some other concepts, always when used in an ISSRM context, are generalisations of ISSRM concepts:

- Security requirements are specific instances of *Requirement*.
- Risk is a specific instance of *Measure*.
- Security criterion is a specific instance of *Driver*
- Security objective is a specific instance of *Goal* or *Objective*.

Finally, some EAM concepts of TOGAF have been identified as related to concepts of the ISSRM domain model:

- *Assumption, Constraint, Principle,* as well as *Role* and *Organization Unit* that are external to the IS (represented as *ext_Role* and *ext_Organization unit* in Fig. 1) are part of the environment of the assets studied. A new concept entitled "Environment" has been added to the model and is composed of the preceding concepts.

The resulting EAM-ISSRM integrated model is shown in Fig. 1. It lies on the ISSRM domain model, depicting the state-of-the-art concepts of ISSRM, and is improved with EAM concepts, represented by black boxes with white names. In summary, a refinement of Business and IS assets has first been added, allowing to better model the complexity of current targets of ISSRM. Second, concepts related to the environment of the IS and thus to context establishment requirements have also been added. It helps to avoid that organizations provide insufficient ISSRM reports by bypassing some fundamental aspects of ISSRM, and allows also tackling our challenge of dealing with regulatory pressure involving ISSRM requirements.

5 Related Work

The Open Group, in a white paper published in 2015 [11], analyses different approaches to modelling enterprise risk, as well as security concepts, based on ArchiMate 2.1. However, the scope of this white paper differs from our scope because they also consider non-security related risks (strategic, financial, project, etc.) with information security risks (i.e. risks harming confidentiality, integrity and availability of information). Barateiro et al. [12] propose an alignment between Risk Management, Governance and Enterprise Architecture activities in order to provide a systematic support to map and trace identified risks to artefacts modelled within an EA. Innerhofer-Oberperfler and Breu [13] propose an approach for the systematic assessment and analysis of IT-related risks in organizations and projects. The goal of the approach is to bridge the different views of the stakeholders involved in security management. SABSA [14] is a methodology for developing risk-driven enterprise information security and information assurance architectures and for delivering security infrastructure solutions that support critical business initiatives. The methodology relies on the SABSA model, which is based on the Zachman framework

[3] adapted somewhat to a security view. Goldstein and Franck have proposed a set of 23 requirements a modelling approach should satisfy to deal with IT security design and management [15]. We share the common objective to define a Domain Specific Modelling Language (DSML) enhancing an existing method for enterprise modelling. Their scope is wider as ours, but includes some basic and relevant aspects related to ISSRM. The CORAS approach is a model-driven approach in the sense that graphical models are actively used throughout the whole risk analysis process to support the various analysis tasks and activities, and to document the results [16]. However, CORAS introduces its own kinds of diagrams and does not rely on EAM models to perform ISSRM. As a conclusion, all of the preceding research works are providing some initial and promising inputs towards leveraging EAM to deal with security and/or RM issues. However, to the best of our knowledge, there is no extensive and mature research work trying to benefit from research in EAM to improve RM in the specific field of information security and proposing a complete and fully integrated conceptual model of both domains.

6 Conclusions and Future Work

In this paper, we have described how we developed an integrated EAM-ISSRM conceptual model based on the ISSRM domain model and the TOGAF standard. First, we have analysed the concepts of TOGAF with regards to the concepts of the ISSRM domain model. The result of this analysis is presented under the form of a conceptual alignment table [10], highlighting the relations between the concepts of TOGAF and those of the ISSRM domain model. After having performed this alignment, the key conclusions are summarised, and then, an integrated EAM-ISSRM conceptual model has been established.

As mentioned in the introduction, our work is part of a larger project, and is not limited to TOGAF, that is only one relevant EAM approach. Other references from the EAM literature will also be taken into account to be representative of the domain. To facilitate a high acceptance level of our extension by practitioners, we plan to focus on conceptual models that are used in practice. The EAM-ISSRM conceptual model will be iteratively improved when considering additional references. Then, after having established an integrated EAM-ISSRM conceptual model based on a representative set of references, it is necessary to validate the results obtained. To do so, we plan to get information about the utility and usability [17] of the EAM-ISSRM integrated model by means of a validation focus group.

Acknowledgments. Supported by the Luxembourg National Research Fund, and financed by the ENTRI project (C14/IS/8329158).

7 References

1. Mayer, N.: Model-based Management of Information System Security Risk, (2009).

2. ISO/IEC 27005:2011: Information technology – Security techniques – Information security risk management. International Organization for Standardization, Geneva (2011).
3. Zachman, J.A.: A framework for information systems architecture. IBM Syst. J. 26, 276–292 (1987).
4. Saha, P. ed: A Systemic Perspective to Managing Complexity with Enterprise Architecture: IGI Global (2013).
5. Lankhorst, M.: Enterprise Architecture at Work - Modelling, Communication and Analysis. Springer Berlin Heidelberg (2013).
6. Dubois, E., Heymans, P., Mayer, N., Matulevičius, R.: A Systematic Approach to Define the Domain of Information System Security Risk Management. In: Nurcan, S., Salinesi, C., Souveyet, C., and Ralyté, J. (eds.) Intentional Perspectives on Information Systems Engineering. pp. 289–306. Springer Berlin Heidelberg, Berlin, Heidelberg (2010).
7. Mayer, N., Grandry, E., Feltus, C., Goettelmann, E.: Towards the ENTRI Framework: Security Risk Management enhanced by the use of Enterprise Architectures. In: Advanced Information Systems Engineering Workshops. Springer International Publishing (2015).
8. The Open Group: TOGAF Version 9.1. Van Haren Publishing, The Netherlands (2011).
9. Zivkovic, S., Kuhn, H., Karagiannis, D.: Facilitate Modelling Using Method Integration: An Approach Using Mappings and Integration Rules. In: Proceedings of the 15th European Conference on Information Systems (ECIS 2007) (2007).
10. Mayer, N., Aubert, J., Grandry, E., Feltus, C., Goettelmann, E.: An Integrated Conceptual Model for Information System Security Risk Management and Enterprise Architecture Management based on TOGAF, ArchiMate, IAF and DoDAF. Technical Report. Available on demand. (2016).
11. Iver Band, Wilco Engelsman, Christophe Feltus, Sonia González Paredes, Jim Hietala, Henk Jonkers, Sebastien Massart: Modeling Enterprise Risk Management and Security with the ArchiMate® Language. The Open Group (2015).
12. Barateiro, J., Antunes, G., Borbinha, J.: Manage Risks through the Enterprise Architecture. In: 45th Hawaii International Conference on System Science (HICSS). pp. 3297–3306 (2012).
13. Innerhofer-Oberperfler, F., Breu, R.: Using an Enterprise Architecture for IT Risk Management. Presented at the Information Security South Africa 6th Annual Conference (2006).
14. John Sherwood, Andrew Clark, David Lynas: SABSA ® Enterprise Security Architecture, (2010).
15. Goldstein, A., Frank, U.: A Language for Multi-Perspective Modelling of IT Security: Objectives and Analysis of Requirements. In: La Rosa, M. and Soffer, P. (eds.) Business Process Management Workshops. pp. 636–648. Springer Berlin Heidelberg (2013).
16. Bjørnar Solhaug, Ketil Stølen: The CORAS Language - why it is designed the way it is. In: Safety, Reliability, Risk and Life-Cycle Performance of Structures and Infrastructures. pp. 3155–3162. CRC Press (2014).
17. Nielsen, J.: Usability Engineering. Morgan Kaufmann (1994).