Conceptual Integration of enterprise architecture management and security risk management

Grandry, Eric; Feltus, Christophe; Dubois, Eric

Published in:
Proceedings of the Fifth Workshop on Service oriented Enterprise Architecture for Enterprise Engineering (SoEA4EE'2013), an International Workshop of the 17th IEEE International EDOC Conference (IEEE EDOC 2013)

DOI:
10.1109/EDOCW.2013.19

Publication date:
2013

Document Version
Early version, also known as pre-print

Link to publication

Citation for pulished version (HARVARD):
Grandry, E, Feltus, C & Dubois, E 2013, Conceptual Integration of enterprise architecture management and security risk management. in *Proceedings of the Fifth Workshop on Service oriented Enterprise Architecture for Enterprise Engineering (SoEA4EE'2013), an International Workshop of the 17th IEEE International EDOC Conference (IEEE EDOC 2013).* IEEE Computer society, pp. 114-123. https://doi.org/10.1109/EDOCW.2013.19

Conceptual Integration of Enterprise Architecture Management and Security Risk Management

Eric Grandry, Christophe Feltus, Eric Dubois
Service Science and Innovation
CRP Henri Tudor
Luxembourg
{eric.grandry, christophe.feltus, eric.dubois}@tudor.lu

***Abstract*—Enterprise Architecture Management (EAM) is considered to provide the mechanism for, amongst others, governing enterprise transformations required by changes in the environment. In this paper, we focus on changes that result from the analysis of information security risks and of their impacts on the services delivered by an enterprise. We present how the concepts of an information system security risks management domain can be mapped into the ArchiMate enterprise architecture modeling language. We illustrate the application of the proposed approach through the handling of a lab case.**

Keywords—EAM, Information Security Risk Management, ArchiMate, Enterprise Model Integration.

I. Introduction

To remain competitive in the growing services economies, enterprises have to transform themselves in business service oriented enterprises. Business services are delivered by service system defined as "a configuration of people, processes, technology and shared information connected through a value proposition with the aim of a dynamic co-creation of value through the participation in the exchanges with customers and external/internal service systems" [1]. According to this view, a service system can be composed of service systems, cooperating to produce the business service. It is typically observed in value constellation like a cloud ecosystem, where the final user of the cloud service (whether IaaS, PaaS or SaaS) depends on a chain of business partners.

The value proposition of a service system can be refined into a number of requirements characterizing the expected qualities of the business services. Usually a distinction is made between functional and non-functional requirements. In this paper, we investigate a specific type of non-functional requirements which are those related to security qualities associated with information delivered through business services. Today, many business services are information intensive and thus security requirements like e.g. information confidentiality or privacy are essential. According to the usual requirements engineering terminology [26, 27], we call "security goals" these requirements in the rest of the paper. The sources for these security goals are customers' needs (e.g. need for confidentiality of the information stored on the cloud) but also, in an increased regulated market, the compliance with regulations and norms (e.g. the compliance with privacy of information manipulated by the service provider). The achievement of security goals associated with the business services delivered by a service system is heavily depending on the quality of the Information System (IS) implementing it. Thus the alignment of the deployed information system with the business perspective is a key issue.

One of the main purposes of Enterprise Architecture Management (EAM) is to align an enterprise to its requirements and business goals, and specifically in our context business services goals. EAM helps to design and guarantee a coherent enterprise's organizational structure, business processes, and infrastructure [2] through a set of models. It transforms enterprise governance into informed enterprise governance [3]. The occurrence of security breaches (for example the corruption of a database) may result in deviations (misalignments) between the business goals of the enterprise and their realization in terms of its implemented information system. The solutions to overcome these misalignments are more and more complex and it is not always either technically or economically sustainable for an enterprise to solve all the potential breaches. Risk Management (RM) as a decision tool therefore becomes a central activity in the design of the architecture components (the so-called "counter-measures") preventing these misalignments.

There exist many Information System Security Risk Management (ISSRM) approaches for analyzing and managing the potential security breaches. The first objective of the paper is to report about our contribution in an extended EAM supporting a security risk-oriented design of an Enterprise Architecture (EA), meeting its associated business services security goals. The core of the framework relies on the integration of ISSRM concepts into EA constructs with a service system perspective.

The second objective of the paper is to address the representation of the performed security risk analysis. A large majority of existing ISSRM approaches are based on the production of textual information, some of them being structured in tabular forms. Thus in general they lack from formal notation and representation. Moreover the traceability between the different elements of the risk model is also difficult to manage. To overcome these difficulties, our proposed extended EAM is embedded in the ArchiMate modeling language [4]. ArchiMate has been purposely designed for supporting EAM, and recent extensions include constructs supporting the service-oriented enterprise. Our proposal aims at using it in conjunction with concepts of information security risks analysis. Of a particular interest is the Business Motivation Model, which we use through the ArchiMate Motivation Extension, for expressing the specific risk analysis related motivations for architecture principles and decisions.

The rest of the paper is structured as follows. In section II, we provide some background knowledge regarding our proposed extended EAM. On the one hand, this includes an introduction to a previous research work performed at the Tudor Centre with respect to the definition of a domain model associated with the concepts that can be found in security risks analysis methods. On the other hand we recall the modeling concepts available in the ArchiMate language and emphasize motivational elements included in the ArchiMate Motivation Extension. In Section III the core of the proposed extended EAM is presented through the study of the mapping that can be made between the security risk metamodel concepts and those of the ArchiMate metamodel. This mapping is done within the perspective of service oriented EA. By doing so, we explain how security risks concepts can be embedded in the ArchiMate language. We illustrate the result of this embedding in Section IV where we apply the proposed security extended EAM in the context of a case study and show how its application can be captured in terms of an ArchiMate model. Section V reviews existing approaches with similar research objectives and Section VI concludes with some future perspectives regarding the positioning of our work.

II. Background Knowledge

In this section, we introduce our two main sources of knowledge on which our research built upon, namely a conceptual security risk model and the ArchiMate language.

A. *Risk Management*

Information System Security Risk Management (ISSRM) is paramount because it helps companies to adopt cost-effective security measures. Indeed, security threats are so numerous that it is impossible to act on all of them because (1) every technological security solution has a cost, and (2) companies have limited resources. Hence, companies want to make sure that they adopt only solutions for which the Return On Security Investment (ROSI) is positive. This is done by comparing the cost of a solution with the risk of not using it, e.g. the cost of a business disruption due to a successful security attack.

There exist a lot of ISSRM approaches. One of the main problems is that they all rely on different concepts and terminologies. Despite efforts started at the standardization level, there is still a need for a common unifying set of concepts. In a previous research performed at Tudor Centre, the different concepts of ISSRM and their relationships have been formalized under the form of a domain metamodel (Fig. 1), i.e. a conceptual model depicting the studied domain [5], [6]. The ISSRM domain model has been established through the analysis of the related literature: risk management standards [7], [8] security-related standards [9], [10] security risk management standards [11]-[14] and methods [15]-[19] and security requirements engineering frameworks [20]-[22].

The ISSRM domain model is organized in three groups of concepts, as represented on Fig. 1:

- Asset-related concepts describe assets and the goals which guarantee asset security.
- Risk-related concepts present how the risk itself is defined.
- Risk treatment-related concepts describe what decisions, requirements and controls should be defined and implemented in order to mitigate possible risks.

In this paper, we use the concept of Security Goal, which merges the concepts of Security Criterion and Security Objective defined in the initial model.

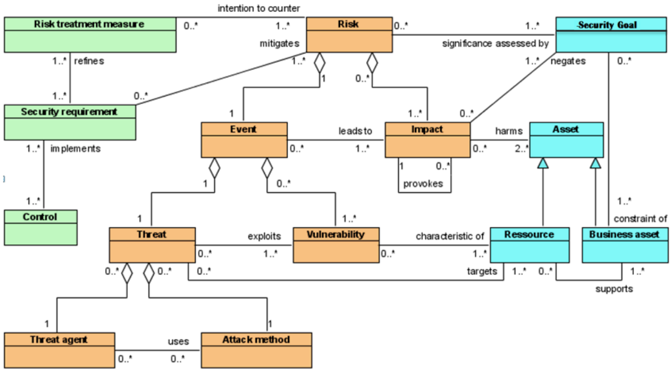

Fig. 1. ISSRM domain model (extracted from [5])

The description of the main concepts of the ISSRM domain model is summarized in TABLE I.

TABLE I. ISSRM Concepts (extracted from [5])

Concept	Description
Asset	Anything that has value to the organization and is necessary for achieving its objectives
Business Asset	Describes information, processes, capabilities and skills inherent to the business and core mission of the organization, having value for it
IS Asset	A component of the IS supporting business assets like a database where information is stored
Security Goal	A property or constraint on business assets describing their security needs, usually for confidentiality, integrity and availability
Risk	The combination of a threat with one or more vulnerabilities leading to a negative impact harming the assets
Impact	The potential negative consequence of a risk that may harm assets of a system or an organization, when a threat (or the cause of a risk) is accomplished
Vulnerability	A characteristic of an IS asset or group of IS assets that can constitute a weakness or a flaw in terms of IS security
Threat	A potential attack or incident, which targets one or more IS assets and may lead to the assets being harmed
Risk Treatment	An intentional decision to treat identified risks
Security Requirement	The refinement of a treatment decision to mitigate the risk
Control	Controls (countermeasures or safeguards) are designed to improve security, specified by a

Concept	Description
	security requirement, and implemented to comply with it

The ISSRM domain model is neutral with respect to the types of business, of industries and sectors. In section III, we will discuss of its specialization with respect to the service sector.

B. EAML and ArchiMate

The Open Group proposes ArchiMate as a standard Enterprise Architecture Modeling Language (EAML), which provides the capability to represent an enterprise in a uniform way, according to the multiple stakeholders' viewpoints, across business, IS and IT architecture layers [2]. Although it has not been specifically developed for the service system domain, ArchiMate introduces constructs supporting the concept of service as an abstraction of the behavior exposed by a system [4]. In enterprise engineering, an enterprise is viewed as a complex designed system, and a service-oriented enterprise can therefore be considered as a set of services exposed to the enterprise's environment.

ArchiMate introduces a layered representation of the enterprise architecture, organized in 3 abstraction layers: business, application and technology. The layers conform to strict dependencies going from upper layer (business) to bottom layer (infrastructure), i.e. the elements of the business layer have dependencies on elements of the application layer, which have dependencies on elements of the technology layer. There are no dependencies permitted the other way round.

The modeling pattern exposed in Figure 2 forms the foundation of the language: a service at the same time abstracts a behavior (that realizes the service) and is a part of a behavior (composed of services). The pattern is instantiated in each abstraction layer, contextualized with the relevant concepts of that layer introducing the concepts of business service, application service and infrastructure service.

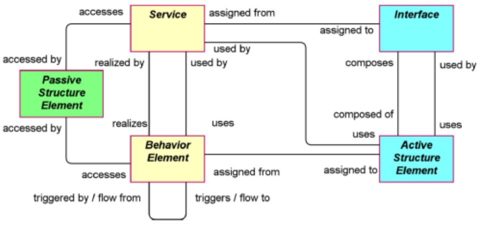

Fig. 2. ArchiMate modeling pattern (extracted from [4])

Two extensions have been introduced in the version 2.0 of the language specification: the Motivation extension and the Implementation and Migration extension. The Motivation extension (Fig. 3) defines the motivational element, abstracting "the reason lying behind the architecture of an enterprise". A motivational element is related to a core element of the architecture through the concept of requirement: a requirement is realized by a (set of) core elements of the architecture. The motivation extension has been developed to support an additional dimension of the architecture: besides the what (passive structure), who (active structure) and how (behavior), the motivation supports the why dimension. The motivation is relevant in each of the 3 abstraction layers (business, application and technology) and allows tracing the rationale behind the elements of the architecture.

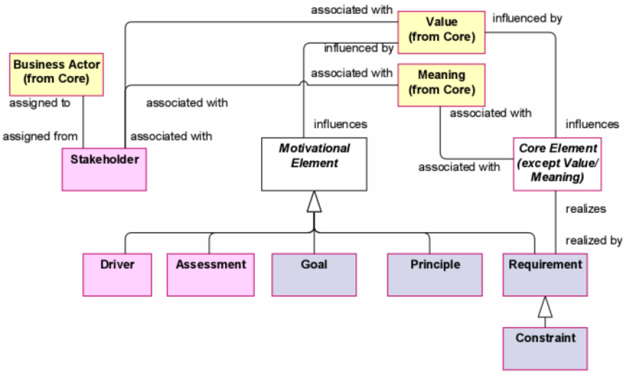

Fig. 3. ArchiMate Motivation Extension (extracted from [4])

The definition of the main concepts of the ArchiMate metamodel is summarized in TABLE II.

TABLE II. ARCHIMATE CONCEPTS (EXTRACTED FROM [4])

Concept	Description
Business Service	A service that fulfills a business need for a customer (internal or external to the organization).
Business Object	A passive element that has relevance from a business perspective.
Business Process	A behavior element that groups behavior based on an ordering of activities. It is intended to produce a defined set of products or business services.
Business Actor	An organizational entity that is capable of performing behavior.
Business Role	The responsibility for performing specific behavior, to which an actor can be assigned.
Application Service	A service that exposes automated behavior.
Application Component	A modular, deployable, and replaceable part of a software system that encapsulates its behavior and data and exposes these through a set of interfaces.
Data Object	A passive element suitable for automated processing.
Infrastructure Service	An externally visible unit of functionality, provided by one or more nodes, exposed through well-defined interfaces, and meaningful to the environment.
Node	A computational resource upon which artifacts may be stored or deployed for execution.
Device	A hardware resource upon which artifacts may be stored or deployed for execution.
Network	A communication medium between two or more devices.
System Software	A software environment for specific types of components and objects that are deployed on it in the form of artifacts.
Artifact	A physical piece of data that is used or produced in a software development process, or by deployment and operation of a system.
Value	The relative worth, utility, or importance of a business service or product.
Driver	Something that creates, motivates, and fuels the change in an organization.
Assessment	The outcome of some analysis of some driver.
Goal	An end state that a stakeholder intends to achieve.

Concept	Description
Requirement	A statement of need that must be realized by a system.
Principle	A normative property of all systems in a given context, or the way in which they are realized.

III. Mapping of Concepts

The purpose of our research is to build an extended EAM supporting a security risk-oriented design of an EA meeting its associated business services goals. This extended EAM is the result of the integration of ISSRM and EAM through the Enterprise Model Integration (EMI) approach [23], [24]. Given the two metamodels to integrate (ArchiMate and ISSRM), we concentrate on resolving the semantic heterogeneity through concept mapping and integration rules [25]: neither the syntactical nor the structural heterogeneity is indeed relevant in our case, as the ISSRM metamodel does not currently propose any concrete syntax. A concept mapping introduces a correspondence between at least one concept of each of the source model. The major correspondences are: Equivalence, Relation and Non-Relation. A relation between two concepts can be a generalization (and reversely specialization), a composition, an aggregation, an association, a classification. While the concept mapping addresses what is integrated, the integration rules addresses how the integration is actually performed, depending on the defined mapping. Equivalent concepts are integrated through an alignment rule (merge, mapping, abstraction), while related concepts are integrated through a connection rule (generalization, aggregation, composition, association, classification).

In this paper, we specifically develop the mapping of concepts between both metamodels, also encompassing the service dimension. The result of the application of the integration rules is only briefly illustrated.

A. Asset-Related Concepts

The ISSRM distinguishes between business assets and IS assets (resources), as exposed in Section II. Security risk management practitioners usually classify business processes, information, skills and capabilities as business assets. We apply this classification and consider that in EAM, a Business Process, a Business Object, a Business Actor and a Business Role are all business assets. These elements deliver Value through the central concept of Business Service: information, business processes and skills are leveraged for the service-oriented enterprise to deliver its value (through the business service). The Business Service encapsulates these business assets and abstracts the value they bring to the enterprise.

We therefore introduce the first mapping of concepts: a Business Process, a Business Object, a Business Actor and a Business Role, all are specializations of a Business Asset in terms of risk management.

The concept of IS Asset in ISSRM abstracts a component of the IS that support the business asset. It is very close to the EAM domain that considers that elements of the application layer realize (or are used by) the elements of the business layer. Application and infrastructure services are the major abstractions of the application and technology layers. They are however not sufficient to be considered in the mapping of the IS Asset in terms of risk management: the vulnerabilities are indeed not the characteristics of the packaged set of resources (which the service abstracts), but of the actual components that the service is made of, i.e. of the structural elements of the technology architecture.

A second mapping of concepts is therefore introduced in the form of specialization between the structural elements of the technology and application layers and the IS Asset concept of ISSRM: a node, a device, a system software, a network and an application component, all are specialization of IS Asset. This means that the vulnerabilities of all these elements need to be identified in a risk assessment exercise.

B. Risk-Related Concepts

A Security Goal represents an intention of securing the business assets in order to increase the value of the associated business service. For example, the confidentiality of the information manipulated by the business service increases the value of the service when it is relevant for the business. Although it could be tempting associating the Security Goal with a goal in terms of EAM, it is important to remind that risk management defines the Security Goal as an indicator to assess the significance of the risks. We therefore choose to map the Security Goal to the concept of Driver in terms of EAM (a Security Goal is-a Driver), and the concept of Risk to the concept of Assessment (a Risk is-a Assessment). The mapping of the relation between Security Goal and Business Asset requires additional concepts to be considered: ArchiMate indeed does not support direct relation between Driver (Security Goal) and the elements of the business layer (Business Asset). However, a Driver influences the Value of a Business Service: the Security Goal associated with a Business Asset influences the value of the Business Service encapsulating these assets, e.g. the confidentiality of the information manipulated by the business service increases the value of the business service in today's context of cloud infrastructure. Given this mapping of concepts, security risk management can therefore be expressed in the following way: the risk is the outcome of the analysis made on the intention to secure business elements of the enterprise in order to increase the value of the associated business service.

The components of the Risk (Event and Impact) are also modeled with the concept of Assessment and the composition relation (an Assessment composed of other Assessments), as they are the results of the risk analysis. The same approach is applied to map the Threat and the Vulnerability.

As explained in Section II, there are causal chains of impacts. Final elements of these chains (like, the loss of reputation) negatively impact the value of one or several business services, through a negative influence on a Driver. We propose modeling the chain of impacts in ArchiMate with a composition of impacts. It should be noted that the final element of a chain of impact might negatively influence another driver than the one that initiated the risk assessment, and even a non-security driver. For instance, the 'Reputation of the Enterprise' is a strategic driver that is not a security goal. It is however negatively influenced by the impact 'loss of reputation' associated with the security risk 'identification theft' associated with the security goal 'Guarantee integrity of information'. It is therefore very relevant to integrate the analysis of security risks as a strategic activity of the enterprise, and not perform it in a silo.

C. *Risk Treatment-Related Concepts*

Risk treatment deals with the decisions and solutions developed to overcome the risks after they have been identified and assessed. The goal of that part of the model is very relevant to EAM as a governing tool.

The Risk Treatment is the decision of how to treat the Risk: retention, reduction, transfer, avoidance. It is mapped to the EAM concept of Goal: the Goal (Risk Treatment) addresses the Assessment (Risk) of the Driver (Security Goal). The Security Requirement is introduced when the Risk Treatment decision is to reduce the risk. The Security Requirement is naturally modeled with the EAM concept of Requirement: they are the means to reach the end, i.e. to realize the Goal. Finally, the Control as the abstraction of the solution that implements the Security Requirement is mapped to a (set of) Core Elements of the architecture: the realization relation between Requirement and Core Element is used to trace the rationale behind the elements of the solution. The solution to a security requirement can be realized by elements of the business layer, application layer and/or infrastructure layer. When multiple solutions can be envisaged, the enterprise architecture models represent a support to take the final decision, potentially based on an ROI analysis.

It should be noted that ArchiMate introduces also the concept of Principle, supporting an indirection between the Goal and the Requirements. It might be very useful in the design of the Security solution that addresses the security risks: the security guidelines that are very common in the security domain (although not part of the ISSRM model) can benefit from this modeling element.

D. *Integrated Metamodel*

The mapping between the concepts of ISSRM and EAM is summarized in TABLE III.

TABLE III. ISSRM-EAM CONCEPTS MAPPING

ISSRM Concept	EAM Concept	Mapping
Business Asset	Business Process	Generalisation
Business Asset	Business Object	Generalisation
Business Asset	Business Actor	Generalisation
Business Asset	Business Role	Generalisation
IS Asset	Application Component	Generalisation
IS Asset	System Software	Generalisation
IS Asset	Node	Generalisation
IS Asset	Device	Generalisation
IS Asset	Network	Generalisation
Security Objective	Driver	Specialisation
Risk	Assessment	Specialisation
Event	Assessment	Specialisation
Impact	Assessment	Specialisation
Threat	Assessment	Specialisation
Vulnerability	Assessment	Specialisation
Risk Treatment	Goal	Specialisation
Security Requirement	Requirement	Specialisation
Control	Core Element	Specialisation

Once the concepts are mapped, the rules (how) to integrate the concepts within the integrated metamodel are defined. The concepts are mainly mapped through generalisation (or specialisation) relation and we apply the related generalisation (or specialisation) integration rule. When it comes to adopt a representation of the risk concepts (concrete syntax) within the integrated model, we decide at this stage to reuse the existing ArchiMate notation: a Security Goal is a Driver, and reuses the Driver symbol as representation. A part of the resulting integrated metamodel is illustrated in Fig. 4, in the ArchiMate notation.

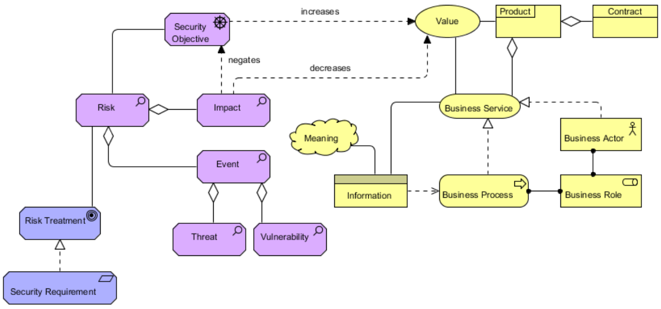

Fig. 4. ISSRM in Relation with EAM

IV. CASE STUDY – @RCHIMED

The metamodel integration is illustrated with a lab case study, @rchimed[1], which is a reference case study for the EBIOS method [15]. This latter is a risk analysis method defined by the French Ministry of Defense which firstly allows evaluating security risks of the IS and secondly allows elaborating appropriate policies according to the organization needs. The description of the case study is organized in two parts. In the first part, we present the context and the existing enterprise architecture of @rchimed. During this part, we identify the assets of the enterprise and we elaborate a standard ArchiMate-based EA model that highlights the connections between the business assets and the IS assets. The second part of the case study concerns the security risk management extension. We model the @rchimed enterprise risks following the mapping realized in Section III.

[1] http://www.ssi.gouv.fr/IMG/pdf/EBIOS-EtudeDeCas-Archimed-2010-01-25.pdf

A. @rchimed architecture

@rchimed is an AEC company specialized in the design of blueprints for the building of new factories and offices. To that end, @rchimed offers, to its customers, services related to the analysis of building stability and estimations of the costs. The reputation of the enterprise is a very important factor to win market shares in a more and more competitive market. @rchimed's strategy is based on two drivers: on one hand improving the reputation of the company, and on the other hand reducing the costs to remain competitive.

We focus on the *studies elaboration* business service, exploited by external *customers*, and achieved by three processes performed by the @rchimed *experts*, namely: the *visualization elaboration*, the *structures calculation* and the *technical plans elaboration*. These processes generate two business objects: the *building structure calculations* and the *structural parameters*. Amongst these processes, the *structures calculation* is supported by the *calculation service* which is itself realized by the *Structure Management Software.* This application is accessed by the experts through the *parameters setting* interface and generates the calculations on *files*, *listings* and *USB* supports. The value of the *studies elaboration* business service relies upon the accuracy of the delivered product (to know: the *structural parameters* business object). This part of @rchimed has been modeled with ArchiMate and presented on the left top part of Figure 5. Regarding the management of the risks, we consider, that the *studies elaboration* business service corresponds to the business asset and that the *Structure Management software* application and *parameters setting* interface correspond to the IS assets.

B. Risk management

This second part of the case study corresponds to the deployment of a classical risk analysis that we have addressed through 3 steps (according to ISO 27005 [12]): definition of the security goals, analysis of the risks and definition of the risks treatment.

1) Definition of the security goals

In order to support and increase the value of its *studies elaboration* business service, @rchimed identifies that from a security perspective it is of paramount importance to guarantee the integrity of the calculation (more than its availability or confidentiality). In terms of ArchiMate model, the security goal *integrity of calculation* is therefore modeled as a driver positively influencing the value of the business service *studies elaboration*.

2) Risk analysis

The second step of the analysis consists in determining the security risks and assessing them from the perspective of the identified security goal. Regarding the *integrity of the calculation* goals, the risk is naturally to have *calculation alteration.* This latter could happen following an *identity theft* due to a *lack of access control* on the information system. This risk has an impact on the *loss of integrity*, and according to a chain of impacts on the *loss of reputation, the stability of building not guaranteed, building collapse, lawsuits*.

In terms of ArchiMate model, the *calculation alteration* is a risk modeled with the assessment construct. This assessment is a combination of two other assessments which correspond respectively to the impact and the event. In our case the impact is the *loss of integrity* as well as the chain of impacts (modeled as aggregated assessments), and the event corresponds to the *identity theft*. In the same way, the event is an assessment supported by a combination of two other assessments corresponding to the threat and to the vulnerability. According to the case study, these latter are, namely, the *identity theft* and the *lack of access control*. This lack of access control is a vulnerability that may be exploited when the *expert* introduces *the structural parameters* in the *parameters setting interface*: the vulnerability is characteristic of this interface, while the threat targets the *expert* actor.

The impact *loss of integrity* negates the initial security goal *integrity of the calculation* and therefore has a negative influence on the value of the associated service. Moreover, the deduced impacts also have negative impacts for the strategy of the company: the *loss of reputation* negatively influences the strategic driver *reputation of @rchimed*, while the *lawsuit* negatively influences the strategic driver *reduce costs*.

This second step of the case study highlights that it is possible with the ArchiMate language to identify the risks associated to (security) goals and to describe them in terms of impact, event, threat and vulnerability. However, the ArchiMate language does not allow relating the assessment concept to the core concepts with anything else than the very weak association relation. Thereby, it does not allow strongly typing the relation between the vulnerability and threat concepts with the core EAM concepts.

C. Risk treatment

The threat composing the *calculation alteration* risk being identified as a potential *identity theft*, a risk treatment action has to be undertaken. Although @rchimed is looking for cost reduction, the impacts of this risk are too high for the company to live with it. The risk treatment decision could typically be supported with a cost-impact analysis. @rchimed decides for a risks reduction action associated with the deployment of an access right management. This control should guarantee the *integrity* of the *parameters settings* interface.

This risk treatment is mapped on the concept of goal from the EAML and influences the value of *confidentiality/integrity* of the *parameter settings* interface. This goal is realized by a security requirement which requests to have an *access right control service*. This security requirement is mapped on the requirement concept from EAML and is realized by an *access control service*. This one is depicted on the left bottom part of Fig. 5. The service is realized by three security processes, namely: the *policy elaboration* (that generates the *Security policies* business object), the *exceptions management* and the *access rights audit*. All these processes are assigned to the *security department* and use the *access right management* application service. This latter is realized by an *access control* application that read the *access control security policy* data object and that collaborates with the *parameters setting interface* in order to control the user's access rights.

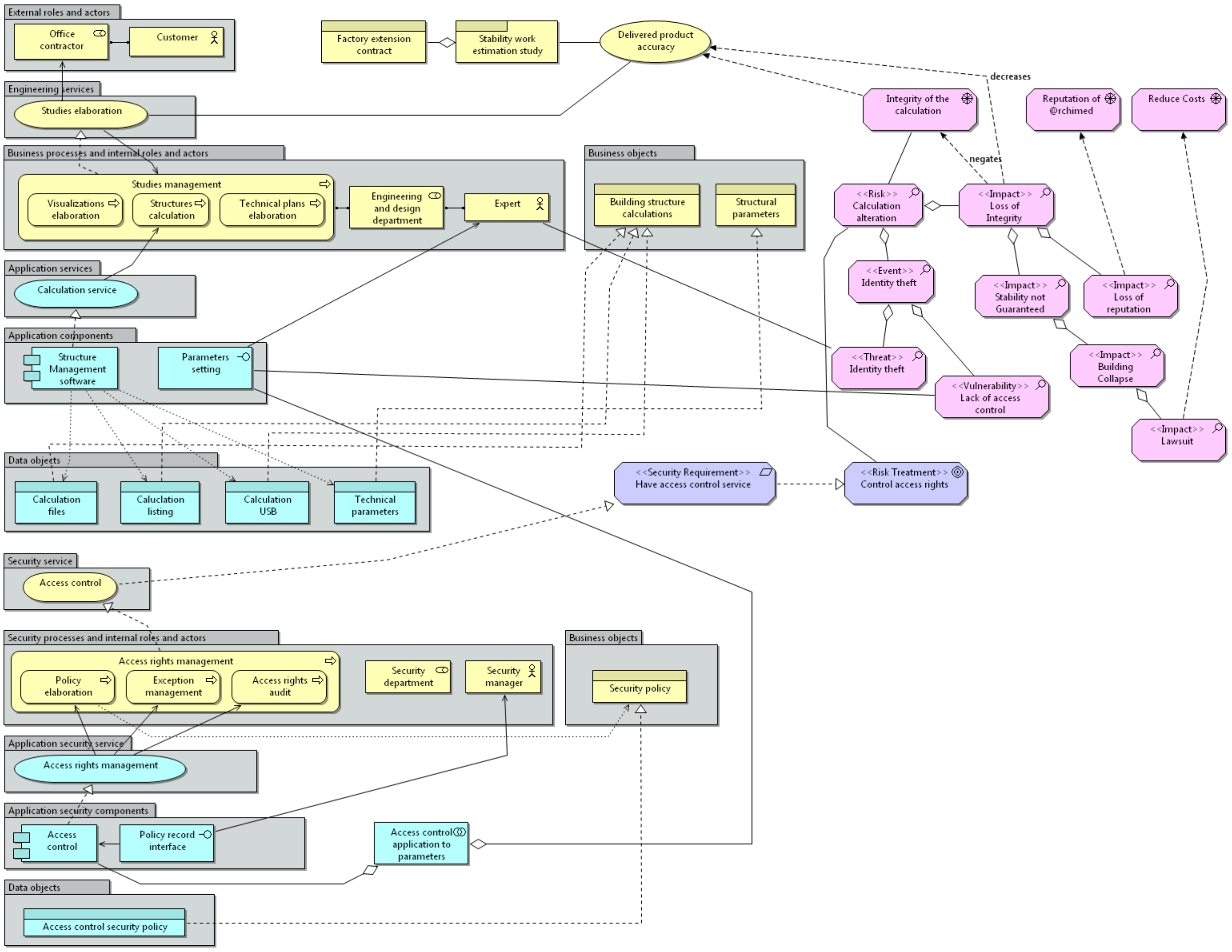
External roles and actors
Office contractor
Customer
Factory extension contract
Stability work estimation study
Delivered product accuracy
decreases
Integrity of the calculation
Reputation of ©rchimed
Reduce Costs
Engineering services
Studies elaboration
Business processes and internal roles and actors
Studies management
Visualizations elaboration
Structures calculation
Technical plans elaboration
Engineering and design department
Expert
Business objects
Building structure calculations
Structural parameters
negates
<<Risk>> Calculation alteration
<<Impact>> Loss of Integrity
<<Event>> Identity theft
<<Impact>> Stability not Guaranteed
<<Impact>> Loss of reputation
<<Threat>> Identity theft
<<Vulnerability>> Lack of access control
<<Impact>> Building Collapse
<<Impact>> Lawsuit
Application services
Calculation service
Application components
Structure Management software
Parameters setting
Data objects
Calculation files
Caluclation listing
Calculation USB
Technical parameters
<<Security Requirement>> Have access control service
<<Risk Treatment>> Control access rights
Security service
Access control
Security processes and internal roles and actors
Access rights management
Policy elaboration
Exception management
Access rights audit
Security department
Security manager
Business objects
Security policy
Application security service
Access rights management
Application security components
Access control
Policy record interface
Access control application to parameters
Data objects
Access control security policy

Fig. 5. @rchimed Extended Enterprise Architecture Model

V. RELATED WORKS

There exist many practical security risks management methods (like BSI, EBIOS, CRAMM, and Octave). However, they lack in formality for their produced analyses which are mostly based on natural language descriptions sometimes complemented with tables and informal diagrams. As stated in [6], the introduction of a model-based approach for ISSRM is relevant. It is motivated first by an efficiency improvement of the ISSRM process, and second by the enhancement of the product resulting of the performed process.

In Requirements Engineering (RE), concepts associated with the analysis and the reasoning on security goals and requirements are introduced in languages like Secure i* [26] addressing security trade-offs, KAOS' extension to security [27], and Secure Tropos [28] extending the language by considering security constraints and attack methods. Abuse cases [29], misuse cases [30] are other RE languages which extend the UML Use Case with a focus on threats and vulnerabilities. In Software Engineering, other extensions to UML have also been proposed for dealing with security issues at the design stages (security requirements and controls), like UMLsec [31] and SecureUML [32] but with less focus on business assets and high-level security requirements.

In the languages mentioned above, only a part of the ISSRM concepts introduced in Section II is taken into account. A larger coverage of the risk related concepts is provided in the UML profile CORAS [33], in another extension of the i* framework [34] and in [35] where a full alignment of Secure Tropos with the ISSRM is presented. Despite these progresses, we argue that theses languages still lack from a crosscutting viewpoint relating all three conceptual areas of risk management together- assets, risks and risk treatments. We advocate that Enterprise Architecture Management (EAM) [3] provides an answer to this by acknowledging that an enterprise is a system that requires modeling from multiple perspectives and at different levels of abstraction. The EAM discipline permits the realization of informed enterprise governance, i.e. enterprise governance based on relevant information. Governance is associated with decision taking and associated risk assessment. Some recent works include the analysis of risks in relation with the business/IT alignment dimension [36] and within the context of the global GRC (Governance, Risk, Compliance) dimension [37]. Our work deepens these results by considering specific information security risks management in the line of [38] but by considering a larger ISSRM metamodel as well as its mapping into ArchiMate

Integrating security risks management and enterprise architecture is also investigated by the ArchiMate forum[2]. The primary objective of this workgroup is to issue a white paper for guidelines about the Risk and Security extensions of ArchiMate. This extension foresees using existing ArchiMate concepts AS-IS to model risk/security aspects, to elaborate risk/security-specific specializations (stereotypes/profiles) and to define new concepts. We take part to this work and expect to leverage the results of the proposed mapping as an input to this activity.

VI. Conclusions and Future Work

In this paper, we have proposed an integration of security risk management and enterprise architecture management in the form of concepts mapping between the metamodels of both domains. The proposed mapping of concepts allows moving further into the integration of risk management and enterprise architecture, especially in terms of method. The benefits of this integration have been illustrated with a case study. The approach leverages enterprise architecture modeling to support the identification of business and IS assets. It also proposes to model the treatment of the risk, especially in relation with the value of the risk treatment and with the rationale behind the elements of the architecture. It however does not give real support in the identification of the threats and vulnerabilities associated with the elements of the architecture: EAML indeed lacks the possibility to express the relations between the risk and assessed element (no direct relationship between Motivational Element and Core Element, at the exception of Requirement). This confirms that the Motivation Extension has been developed to explain the rationale behind the architecture, but not to support analysis of an existing architecture.

The proposed extended EAM also addresses the mechanism to support the service industry with a model of risk that was initially targeting the security of information systems. We are currently investigating the extension of the ISSRM model to apply security risk management to service systems. It is specifically interesting in order to tackle the chain of risks through the networked enterprises.

The extended EAM presented in this paper has been applied in a collaborative R&D project, and more specifically in the definition of a risk management method for the telecommunication sector, in collaboration with the national regulator in Luxembourg. Preliminary results have been presented in [40].

Although requirements to manage risks might be initiated by regulators in all industries, some organizations now consider their risk management capabilities as an opportunity to drive competitive advantage. In its 2011 study on Global Risk Management [39], Accenture identifies that “risk management is now more closely integrated with strategic planning and is conducted proactively, with an eye on how [risk management] capabilities might help a company move into new markets faster or pursue other evolving growth strategies. At its best, risk management is a matter of balance — the balance between a company’s appetite for risks and its ability to manage them”. We assist to the transformation of risk management from an operational regulatory constraint, to a mean to drive strategic enterprise transformation. This new perspective on risk management enforces the need to integrate risk management and EAM.

Acknowledgment

We acknowledge the Fond National de la Recherche (FNR) in Luxembourg that partially supports this work through the PEARL program ASINE. We also thank our colleague Nicolas Mayer for his valuable advises in the field of risk management, and his time spent in very intense discussions around this topic.

References

[1] J. Spohrer, P. Maglio, J. Bailey, D. Gruhl, "Steps toward a science of service sytems". IEEE Computer, 40, pp. 71–77, 2007

[2] M. Lankhorst, *Enterprise Architecture at Work - Modelling, Communication and Analysis*, 3rd ed. Springer Berlin Heidelberg, 2013

[3] M. Op 't Land, Proper, M. Waage, J. Cloo, and C. Steghuis, *Enterprise Architecture - Creating Value by Informed Governance*. Springer Berlin Heidelberg, 2008

[4] The Open Group, *ArchiMate 2.0 Specification*. Van Haren Publishing, The Netherlands, 2012

[5] N. Mayer, “Model-based Management of Information System Security Risk,” PhD Dissertation, University of Namur, 2009.

[6] E. Dubois, P. Heymans, N. Mayer, and R. Matulevičius, “A Systematic Approach to Define the Domain of Information System Security Risk Management,” in *Intentional Perspectives on Information Systems Engineering*, S. Nurcan, C. Salinesi, C. Souveyet, and J. Ralyté, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2010, pp. 289–306.

[7] AS/NZS 4360, Risk management. SAI Global, 2004.

[8] ISO/IEC Guide 73, Risk management – Vocabulary – Guidelines for use in standards. Geneva: International Organization for Standardization, 2002.

[9] ISO/IEC 13335-1, Information technology – Security techniques – Management of information and communications technology security – Part 1: Concepts and models for information and communications technology security management. Geneva: International Organization for Standardization, 2004.

[10] Common Criteria version 3.1, Common Methodology for Information Technology Security Evaluation - Evaluation methodology. 2007.

[11] ISO/IEC 27001, Information technology – Security techniques – Information security management systems – Requirements. Geneva: International Organization for Standardization, 2005.

[12] ISO/IEC 27005, Information technology – Security techniques – Information security risk management. Geneva: International Organization for Standardization, 2008.

[13] G. Stoneburner, C. Hayden, and A. Feringa, NIST Special Publication 800-27 Rev. A: Engineering Principles for Information Technology Security (A Baseline for Achieving Security). Gaithersburg: National Institute of Standards and Technology, 2004.

[2] http://www.opengroup.org/archimate/

[14] Bundesamt für Sicherheit in der Informationstechnik, The IT-Grundschutz Catalogues. 2005.

[15] DCSSI, EBIOS - Expression of Needs and Identification of Security Objectives. France: http://www.ssi.gouv.fr/en/confidence/ebiospresentation.html, 2004.

[16] CLUSIF, MEHARI 2007: Concepts and Mechanisms. France: , 2007.

[17] C. J. Alberts and A. J. Dorofee, "OCTAVE criteria, Version 2.0," Carnegie Mellon University - Software Engineering Institute, Pittsburgh, Pennsylvania, CMU/SEI-2001-TR-016, 2001.

[18] Insight Consulting, CRAMM (CCTA Risk Analysis and Management Method) User Guide version 5.0. SIEMENS, 2003.

[19] F. Vraalsen, T. Mahler, M. S. Lund, I. Hogganvik, F. den Braber, and K. Stølen, "Assessing Enterprise Risk Level: The CORAS Approach," in Advances in Enterprise Information Technology Security, D. Khadraoui and F. Herrmann, Eds. Idea group, 2007, pp. 311–333.

[20] D. G. Firesmith, "Common Concepts Underlying Safety, Security, and Survivability Engineering," Carnegie Mellon University - Software Engineering Institute, Pittsburgh, Pennsylvania, CMU/SEI-2003-TN-033, 2003.

[21] C. B. Haley, R. C. Laney, J. D. Moffett, and B. Nuseibeh, "Security Requirements Engineering: A Framework for Representation and Analysis," IEEE Transactions on Software Engineering, vol. 34, no. 1, pp. 133–153, 2008.

[22] S.-W. Lee, R. A. Gandhi, and G.-J. Ahn, "Security Requirements Driven Risk Assessment for Critical Infrastructure Information Systems," in Proceedings of the 3rd Symposium on Requirements Engineering for Information Security (SREIS ’05), in conjunction with the 13th IEEE International Requirements Engineering Conference (RE ’05), 2005.

[23] Kühn, H., Bayer, F., Junginger, S. and Karagiannis, D. (2003). Enterprise Model Integration. In:Proceedings of the 4th International Conference EC-Web 2003 (DEXA 2003), Czech Republic, 2003, LNCS 2738, Springer, pp. 379-392.

[24] Karagiannis, D. and Kühn, H. (2002). Metamodelling Platforms. In: Proceedings of the Third International Conference EC-Web 2002 – Dexa 2002, Aix-en-Provence, France, September 2-6, 2002, LNCS 2455, Springer-Verlag, p. 182. Full version: http://www.dke.univie.ac.at/mmp

[25] Zivkovic, S.; Kuhn, H.; and Karagiannis, Dimitris, "Facilitate Modelling Using Method Integration: An Approach Using Mappings and Integration Rules" (2007). ECIS 2007 Proceedings. Paper 122. http://aisel.aisnet.org/ecis2007/122

[26] G. Elahi and E. Yu. A Goal Oriented Approach for Modeling and Analyzing Security Trade-Os. In C. Parent, K.-D. Schewe, V. C. Storey, and B. Thalheim, editors, Proceedings of the 26th International Conference on Conceptual Modelling (ER 2007), volume 4801, pages 87{101. Springer-Verlag Berlin Heidelberg, 2007

[27] van Lamsweerde A (2004) Elaborating security requirements by construction of intentional anti-models. In: Proceedings of the 26th international conference on software engineering (ICSE’04), IEEE Computer Society, pp 148–157

[28] H. Mouratidis and P. Giorgini, Secure Tropos: A Security-oriented Extension of the Tropos Methodology, International Journal of Software Engineering and Knowledge Engineering (IJSEKE), vol. 17, no. 2, pp.285-309, 2007.

[29] McDermott J, Fox C (1999) Using abuse case models for security requirements analysis. In: Proceedings of the 15th annual computer security applications conference (ACSAC’99), IEEE Computer Society, pp 55–65

[30] Sindre G, Opdahl AL (2004) Eliciting security requirements with misuse cases. Reqs Eng J 10(1):34–44

[31] Jürjens J (2002) UMLsec: extending uml for secure systems development. In: Proceedings of the 5th international conference on the unified modeling language (UML’02). LNCS, vol 2460. Springer, pp 412–425

[32] Lodderstedt T, Basin D, Doser J (2002) SecureUML: a UML-based modeling language for model-driven security. In: Proceedings of the 5th international conference on the unified modeling language (UML’02), Springer, pp 426–441

[33] Lund, Mass Soldal, Bjørnar Solhaug, and Ketil Stølen. "Risk analysis of changing and evolving systems using CORAS." Foundations of security analysis and design VI. Springer Berlin Heidelberg, 2011. 231-274.

[34] Elahi G, Yu E, Zannone N (2010) A vulnerability-centric requirements engineering framework: analyzing security attacks, countermeasures, and requirements based on vulnerabilities. Reqs Eng J 15(1):41–62

[35] Matulevičius, R.; Mouratidis, H.; Mayer, N.; Dubois, E.; Heymans, P. (2012). Syntactic and Semantic Extensions to Secure Tropos to Support Security Risk Management. Journal of Universal Computer Science, 18(6), (pp. 816-844).

[36] Nurcan, Selmin, Bruno Claudepierre, and Islem Gmati. "Conceptual Dependencies between two connected IT domains: Business/IS alignment and IT governance." Research Challenges in Information Science, 2008. RCIS 2008. Second International Conference on. IEEE, 2008.

[37] Vicente, Pedro, and Miguel Mira da Silva. "A conceptual model for integrated governance, risk and compliance." Advanced Information Systems Engineering. Springer Berlin Heidelberg, 2011.

[38] Innerhofer-Oberperfler, Frank, and Ruth Breu. "Using an enterprise architecture for IT risk management." Information Security South Africa Conference, ISSA. 2006.

[39] Accenture, "Report on the Accenture 2011 Global Risk Management Study." 2011

[40] Mayer, N., Aubert, J., Cholez, H., Grandry, E. "Sector-Based Improvement of the Information Security Risk Management Process in the Context of Telecommunications Regulation", 20th EuroSPI Conference, CCIS in press.