



An integrated conceptual model for information system security risk management supported by enterprise architecture management

Nicolas Mayer¹ · Jocelyn Aubert¹ · Eric Grandry¹ · Christophe Feltus¹ · Elio Goettelmann¹ · Roel Wieringa²

Received: 22 September 2016 / Revised: 21 July 2017 / Accepted: 16 January 2018
© Springer-Verlag GmbH Germany, part of Springer Nature 2018

Abstract

Risk management is today a major steering tool for any organisation wanting to deal with information system (IS) security. However, IS security risk management (ISSRM) remains a difficult process 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. A first step towards a better integration of both domains is to define an integrated EAM-ISSRM conceptual model. This paper is about the elaboration and validation of this model. To do so, we improve an existing ISSRM domain model, i.e. a conceptual model depicting the domain of ISSRM, with the concepts of EAM. The validation of the EAM-ISSRM integrated model is then performed with the help of a validation group assessing the utility and usability of the model.

Keywords Risk management · Security · Enterprise architecture · ArchiMate

1 Introduction

In today's networked world, information system (IS) security and risk management (RM) are required for every organisation that wishes to survive. Whether for purely compliance purposes, business development opportunities, or even governance improvement, organisations tend to implement a security strategy based on an ISSRM (IS security RM)

approach. However, organisations have to deal with pressures that increase the difficulty of managing security risks. Briefly, the main drawbacks identified in traditional ISSRM methods are:

1. Current IS are more and more complex and subject to an increasing number of threats to manage [1,2].
2. Organisations are continuously evolving, including planned evolution and/or unplanned and emergent changes [3].
3. There is a regulatory pressure on organisations involving ISSRM requirements [4–6].
4. It is difficult to have a clear and manageable documentation for ISSRM activities [7].
5. ISSRM methods are generic, leading to a lack of guidelines in the ISSRM process to follow with regard to the variety of contexts of use (existing IS or IS in design, requirements coming from various regulations, from the governing body, etc.) [7].

Classical ISSRM methods [7,8] are thus no more suitable to deal with the complexity of organisations and associated risks in such a context of compliance and governance. Due to these issues, new solutions are required to address security risks.

Enterprise architecture management (EAM) is a promising approach to deal with drawbacks 1–4. EAM has shown to

Communicated by Professor Alexander Pretschner.

✉ Nicolas Mayer
nicolas.mayer@list.lu

Jocelyn Aubert
jocelyn.aubert@list.lu

Eric Grandry
eric.grandry@list.lu

Christophe Feltus
christophe.feltus@list.lu

Elio Goettelmann
elio.goettelmann@list.lu

Roel Wieringa
r.j.wieringa@utwente.nl

¹ Luxembourg Institute of Science and Technology, 5 Avenue des Hauts-Fourneaux, 4362 Esch-sur-Alzette, Luxembourg

² University of Twente, Enschede, The Netherlands

be a valuable and engaging instrument to face enterprise complexity and the necessary enterprise transformation [9, 10]. It offers means to govern enterprises and make informed decisions: description of an existing situation, investigation and expression of strategic direction, analysis of gaps, planning at the tactical and operational level, selection of solutions, and architecture design [11]. In this paper, we propose to integrate EAM with ISSRM, in order to benefit from the capabilities of EAM to deal with enterprise complexity and evolution at the level of risk management. Such a tool-supported integration of EAM and ISSRM will provide, through the link established between enterprise architectures and related identified risks, a better consideration of drawbacks 1 and 2. Moreover, enterprise architectures include explicitly regulations and external requirements and thus tackle the issue of drawback 3. Finally, by introducing a model-based approach of EAM, documentation of ISSRM activities will be highly improved compared to the usual informal text descriptions (drawback 4).

In earlier work, we have integrated the concepts of existing ISSRM standards and methods into a domain model called the *ISSRM domain model* [12]. The goal of our current research work is to improve this model to deal with the above problems, by extending it to a framework (modelling language, method, and tool) that incorporates results from EAM research [13] and that can be used in practice. In this paper, we report on the first step towards the modelling language part of the framework: defining an integrated EAM-ISSRM conceptual model that we will call the *EAM-ISSRM integrated model*. Note that we do not propose a modelling language, but we do define an underlying conceptual model for such a language. This model will also be a key artefact towards the definition of an associated ISSRM method.

The research results presented in this paper intend to improve the management of information security risks by proposing an EAM-ISSRM integrated model validated by a focus group. More specifically, the contribution of this paper includes:

- an explicit integration of EAM in the domain of ISSRM, relying on state-of-practice standards in the field of EAM,
- the formalisation of the integrated conceptual model, represented under the form of a UML class diagram coming with definitions for each concept of the model, that can be used when developing a method and/or language for ISSRM supported by EAM,
- the assessment of the relevance of such a model from a security risk practitioner's perspective.

Together with the problem investigation step reported about earlier [13], our integrated model and its empirical validation is one iteration through a design cycle [14].

The remainder of the paper is structured as follows. In the following section, the background of our work is described: it introduces the ISSRM domain model and ArchiMate, an EAM modelling language used as example later in the paper. Section 3 describes the research method followed to define an integrated EAM-ISSRM conceptual model. Then, Sect. 4 develops the first step of this research method about the selection of EAM literature that is relevant to our purpose. In Sect. 5, we present as illustrative example the conceptual alignment between the concepts of ArchiMate and those of the ISSRM domain model, and then we explain the key findings. The EAM-ISSRM integrated model is proposed in Sect. 6. In Sect. 7, we present a validation by means of a focus group. Section 8 provides a comparison with related work. Finally, conclusions and future work are presented in Sect. 9.

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 domain of information system security risk management [12]. The ISSRM domain model was designed from related literature [7]: risk management standards, security-related standards, security risk management standards and methods, and security requirements engineering frameworks. It is composed of three 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 [7], as represented in Fig. 1.

Asset-related concepts (light-grey boxes, i.e. the right part of Fig. 1) describe assets and the criteria which guarantee asset security. An *asset* is anything that has value to the organisation and is necessary for achieving its objectives. A *business asset* consists of information, processes, capabilities, or skills inherent to the business and core mission of the organisation, and that is of value for it. An *IS asset* is a component of the IS supporting business assets, such as for example a database where information is stored. As described in the ISSRM literature [7], an IS is a composition of hardware, software, network, people, and facilities. A *security criterion* is a security property or constraint, such as for example confidentiality, integrity, and availability. A *security objective* is the application of a security criterion to a business asset (for example, the confidentiality of personal information).

Risk-related concepts (white boxes, i.e. the middle part of Fig. 1) present how the risk itself is defined. A *risk* is the combination of an event with a negative impact harming the assets. An *impact* describes the potential negative con-

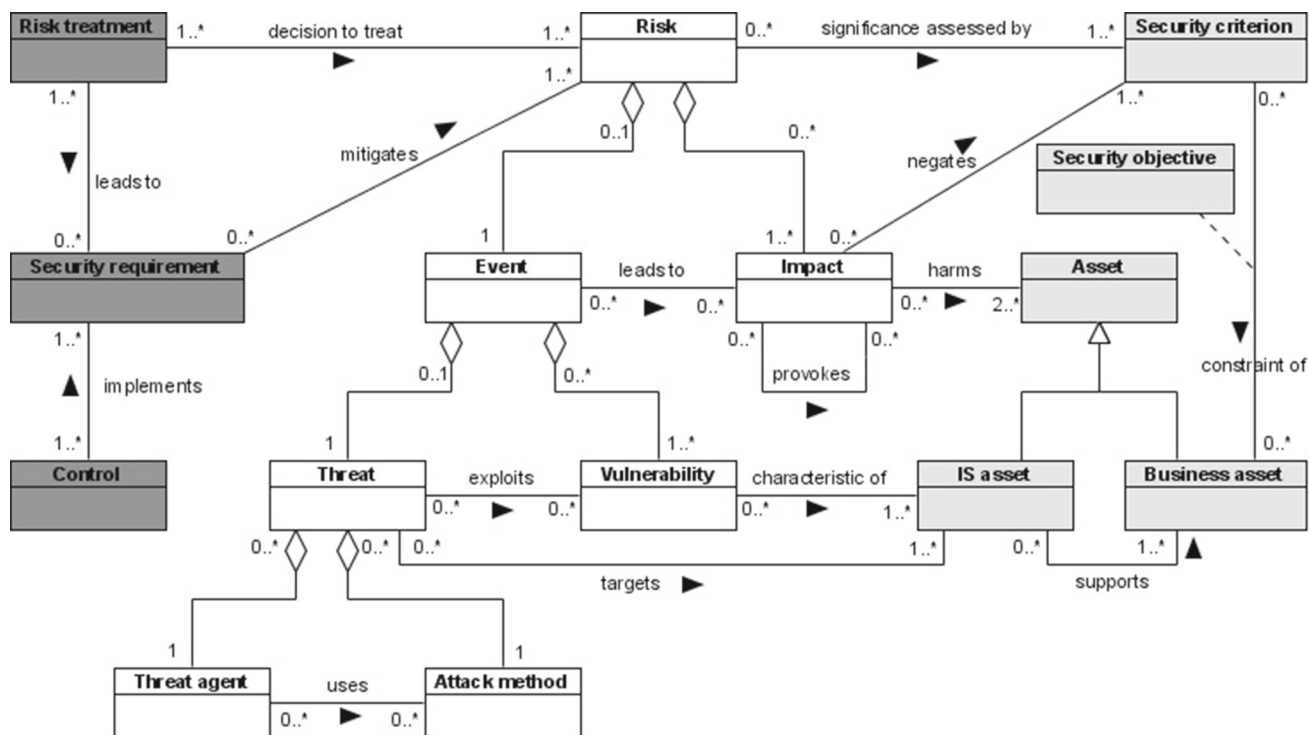


Fig. 1 The ISSRM domain model represented as a UML class diagram (extracted from [7]). Asset-related concepts are represented by light-grey boxes, risk-related concepts by white boxes, and risk treatment-related concepts by dark grey boxes

sequence of an event that may harm assets of a system or organisation, when an event causing this impact occurs. An *event* is the combination of a threat and one or more vulnerabilities. A *vulnerability* is 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* is a potential attack or incident, which targets one or more IS assets and may lead to the assets being harmed. A threat usually 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, i.e. the left part of Fig. 1) 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, such as reducing risks through security requirements, sharing with another party the burden of loss from 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.

We have compared the ISSRM domain model with different security risk modelling languages: Mal-Activity Diagrams [15], Misuse Case [16], Secure Tropos [17], Business Process Modelling Notations [18], and KAOS extended to security [7]. The comparison has shown that none of

these security risk modelling languages support all ISSRM concepts and steps. Each focusses on a limited number of concerns for ISSRM, as discussed in these papers.

2.2 ArchiMate

Enterprise Architecture (EA) is defined as a coherent whole of principles, methods, and models that are used in the design and realisation of an enterprise’s organisational structure, business processes, information systems, and infrastructure [19]. To provide a uniform representation for diagrams that describe EA, the ArchiMate modelling language [20] has been produced by The Open Group, an industry consortium developing standards. It offers an integrated architectural approach to describe and visualise the different architecture domains and their underlying relations and dependencies. The role of the ArchiMate standard is to provide a graphical language for the representation of EA over time, as well as their motivation and rationale. The version of the standard studied in this paper is 2.1, and its evolution is closely linked to the developments of the TOGAF standard [21] and the emerging results from The Open Group forums and work groups active in this area. It is today a widely accepted open standard for modelling EA [22], with a large user base and a variety of modelling tools that support it. The different concepts defined in the language are not introduced in this section, but rather detailed on-the-fly in Sect. 5 where they are analysed.

3 Research method

Following a DSR approach [14], our research method comprises a design task (steps 1–3) and a validation task (step 4). According to the methodology proposed by Peffers et al. [23], our validation task covers demonstration and evaluation tasks. The problem analysis has been performed in the past [13] and is not reported in this paper, but has resulted in the design goal of improving ISSRM by extending it to a framework (modelling language, method, and tool) that incorporates results from EAM research. The scope of this paper is focused on the conceptual model for the modelling language of the framework. The design task extends an existing design, the ISSRM domain model, with EA concepts, and comprises identification of literature on EA, alignment with ISSRM concepts, and integration of EA concepts with the ISSRM domain model to give an integrated model. The artefact to be validated is this integrated model. The validation task is to test if this integrated model is usable and useful for the target group, consisting of ISSRM professionals familiar with the ISSRM domain model, so that the validation is focused on the evolution to the EAM-ISSRM integrated model, the ISSRM domain model as such having already been validated in our previous work [7]. Generalisability to the larger population of all ISSRM professionals is not tested in this study.

In more detail, the research method followed to develop the EAM-ISSRM integrated model is composed of the following steps:

Step 1. Selection of relevant literature on EAM

The first step of the research method consists in selecting relevant literature on EAM that will be used to adapt and extend the ISSRM domain model with EA-related concepts. The literature on EAM is huge, and for our goal it is not necessary to perform a complete review of it. Indeed, to facilitate a high acceptance level of our extension by practitioners, we focus on conceptual models that are used in practice. We describe and motivate our selection in Sect. 4.

Step 2. Conceptual alignment between concepts used to model EA and concepts of the ISSRM domain model

The second step of the research method consists in identifying the semantic correspondence between concepts found in the selected literature on EAM and the concepts of the ISSRM domain model. This task is performed by a design group composed of experts of both domains, in order to consolidate as much as possible the alignment decisions. The approach followed is inspired by Zivkovic *et al.* [24]. 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 A¹;
- *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 for each literature reference on EAM, highlighting the relations between its concepts and those of the ISSRM domain model, and illustrated, when applicable, with an example of use of the EA concepts in an ISSRM context. As a running example, we use a model of a medical analysis laboratory, developed in a national project that aims to improve and facilitate RM in the medical sector. The conceptual alignment step is described in detail in Sect. 5.

Step 3. Design of the EAM-ISSRM integrated model

The third step of our research method consists in designing an integrated EAM-ISSRM conceptual model. This integrated conceptual model is built incrementally, taking into account the different conceptual alignments performed for each studied literature reference in Step 2. More specifically, we build a specific EAM-ISSRM integrated model for each studied literature reference in EAM and reconcile all of them afterwards. The result of this step is described in Sect. 6.

Step 4. Validation of the EAM-ISSRM integrated model

In order to validate the result obtained, we get information about the utility and usability of the EAM-ISSRM integrated model by means of a focus group. This validation group is composed of experienced ISSRM practitioners who answer questions and perform exercises developed for assessing the utility and usability of the model. Members of the validation group are people not involved in the design stage of the EAM-ISSRM integrated conceptual model. We describe our validation and its outcome in Sect. 7.

4 Selection of relevant literature on EAM

The literature on EAM is huge and we need to select the references to be analysed, for integration of EA concepts with those of the ISSRM domain model. To facilitate acceptance in practice, we focus on literature used in industry. More specifically, our scope is on standards (especially ISO and from The Open Group that are particularly active in the EA field) and practitioner methods for EAM.

¹ Generalisation and Specialisation are opposite relations.

The objective of our integrated conceptual model is *to describe the concepts used when defining an EA*. More in particular, the following criteria have been established in order to consider an approach as relevant in our context:

- (a) The approach shall provide information for designing *architecture descriptions*, i.e. the work product used to express an architecture [25].
- (b) The approach shall *clearly describe* the concepts at stake for architectural description, in order to enable a conceptual alignment. Methods that are insufficiently precise at the conceptual level must be set aside. Explicit definitions of the concepts used to describe architectures are required.
- (c) The approach shall allow us to deal with the *architecture of systems* that may consist of hardware, software, data, people, business processes, procedures, facilities, materials, or naturally occurring entities [25,26]. It shall not be restricted to specific kinds of systems (e.g. software products).

Of the approaches listed by existing reviews about EAM [27] or recommended by experts, the following satisfy these criteria:

- ArchiMate, a modelling language introduced in Sect. 2.2. The language metamodel and the definitions for each concept provided in the ArchiMate 2.1 specification [20] have been used as the input for the conceptual alignment work described in the next section.
- TOGAF, a standard established and maintained by The Open Group providing a detailed method and a set of supporting tools for developing an enterprise architecture. The TOGAF Content Metamodel and its associated glossary are the reference used for the conceptual alignment [21].
- DoDAF (standardised in UPDM), a framework and conceptual model to develop architectures to facilitate the ability of Department of Defense (DoD) managers to make decisions. The concepts of DoDAF are described through a set of metamodels that are the reference used for the conceptual alignment [28].
- IAF, an enterprise architecture framework that covers business, information, information system, and technology infrastructure. The Integrated Architecture Content Framework (IACF) and associated definitions of each IAF's artefact are the reference used for the conceptual alignment [29].

At the opposite, the following approaches were considered but rejected, because not satisfying our selection criteria:

- The Zachman framework is defined as the fundamental structure for EA and thereby yields the total set of descrip-

tive representations relevant for describing an enterprise [9]. It focuses on constructing views of an enterprise rather than on providing a process or methodology for the creation of an architecture or architectural description. The Zachman framework does thus not satisfy criterion a and has not been selected although complying with criteria b and c.

- The Open Enterprise Security Architecture (O-ESA) is a guide providing a comprehensive overview of the key security issues, principles, components, and concepts underlying architectural decisions [30]. The guide does not describe concepts (criterion b) nor a framework to define security architectures (criterion a), but only references security architectures (e.g. vulnerability management, asset management) Criteria a and b are thus not satisfied.
- GERAM is a framework about those methods, models and tools which are needed to build and maintain the integrated enterprise, be it a part of an enterprise, a single enterprise or a network of enterprises (virtual enterprise or extended enterprise) [31]. GERAM is a generic framework which does not suggest specific concepts for designing architecture descriptions (criterion a). Explicit definitions are also lacking (criterion b). Criteria a and b are not satisfied.
- The RM-ODP standard is a reference model providing a coordinating framework for the standardisation of Open Distributed Processing (ODP), an ODP relating to the development, use and management of applications distributed across networks of computer systems [32]. The "4+1" view model is a model for describing the architecture of software-intensive systems, based on the use of multiple, concurrent views, and allowing to address separately the concerns of the various stakeholders of the architecture [33]. Both approaches satisfy criteria a and b, but are focused only on software systems and are thus not compliant with criterion c.

To the best of our knowledge, the set of standards and methods considered is representative of the state-of-practice in the field of EAM. We use the four selected approaches as input for designing an extension of the ISSRM domain model including EA concepts. However, we naturally keep open the consideration of other EAM references in the future.

5 Conceptual alignment between concepts of EAM and concepts of the ISSRM domain model

As part of Step 2 of the research method, the four selected EAM methods have been investigated to define the EAM-ISSRM integrated model. However, for the sake of brevity,

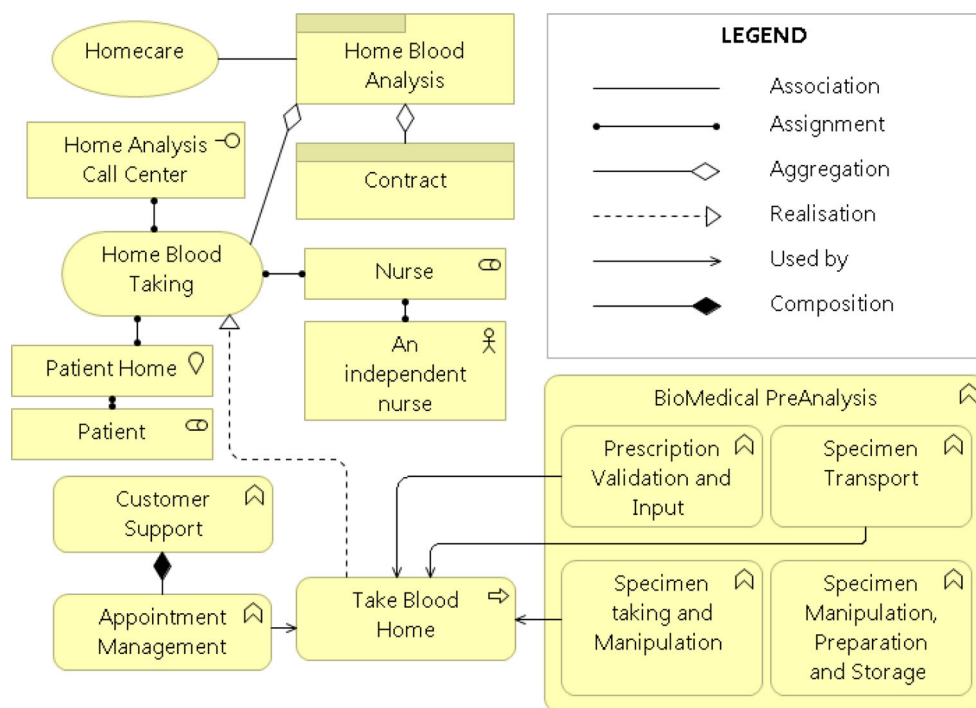


Fig. 2 Business view

this paper reports only part of this work. In this section, we analyse if and how the concepts that are part of ArchiMate [20] can be related to the concepts of the ISSRM domain model. A similar process has been followed for the other three EAM methods [34,35].

Each conceptual alignment has been performed by a design group composed of five people. Three of them are ISSRM experts and two of them EAM experts. All of the members of the design 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 organisations, ranging from SMEs to European institutions). The ArchiMate experts too had practical experience of the use of the language: they used ArchiMate to model enterprise architectures of a dozen of organisations, including the example depicted in this paper. Alignment decisions were taken only once a consensus has been reached among the members of this design group.

5.1 Presentation of the running example

The following case is an excerpt of an EA model of the medical analysis laboratory sector. It has been developed in a national project aiming to improve and facilitate RM in the medical sector [36]. This excerpt, modelled with ArchiMate, details a specific activity of a medical analysis laboratory:

the home blood sample collection. It is organised in four distinct views, namely a Business view (Fig. 2) focussing on business part of “Home Blood Analysis”, a Motivation view (Fig. 3) presenting the value proposition behind the development of “Home Blood Analysis”, an Information view (Fig. 4) presenting information, and finally a Technology view (Fig. 5) focussing on the technological architecture of a specific Business Function. These views were developed to illustrate the majority of the constructs of the three ArchiMate layers, namely the Business Layer, Application Layer and Technology Layer, as well as the Motivation extension, and represented with their standard visual aspect as depicted in ArchiMate 2.1 [20] (see Table 1 for a legend of the nodes of ArchiMate diagrams).

We are aware that this case does not cover all of the studied concepts; however, the case is realistic, and it allows to illustrate as much as possible the alignment achieved. We have performed the concept alignment based on the definitions of the concepts from the specification of ArchiMate [20], and not only on the basis of this example. The example is used only to illustrate the use of ArchiMate constructs (which are very generic) in a context of ISSRM.

The Business view (Fig. 2) is focussed on “Home Blood Analysis” as a product proposed by the laboratory to its patients. This product is composed of *Business Processes* (e.g. “Take Blood Home”), *Business Services* (e.g. “Home Blood Taking”), *Business Functions* (e.g. “BioMedical PreAnalysis”), *Business Roles* (e.g. “Nurse”), *Business*

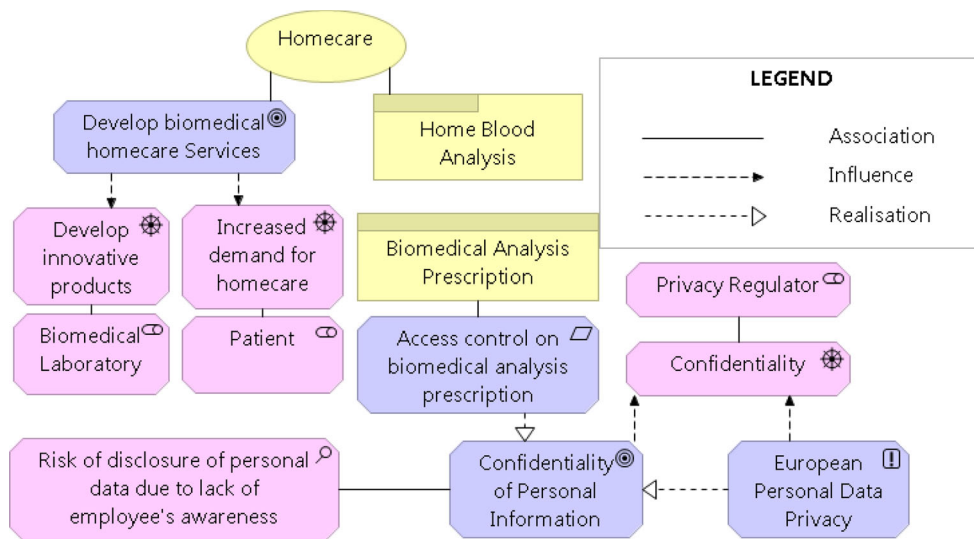
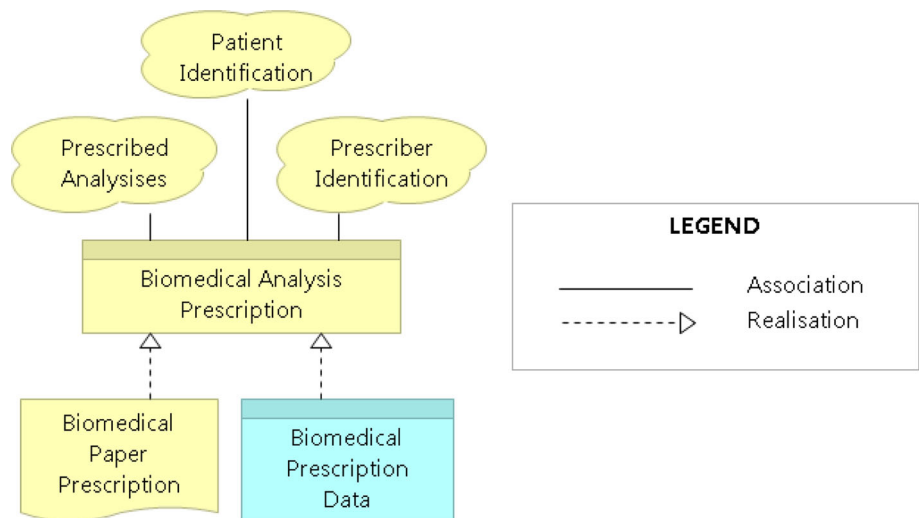


Fig. 3 Motivation view

Fig. 4 Semantic view



Actor (e.g. “An independent nurse”), Location (e.g. “Patient Home”) and Business Interfaces (e.g. “Home Analysis Call Center”). This view proposes a cutting up of the Product in terms of Business Services, performed by Business Roles played by Business Actors. A little further down, Business Services are broken down into Business Functions or groups of Business Functions (e.g. “BioMedical PreAnalysis”).

The Motivation view (Fig. 3) introduces the following concepts: Stakeholder (e.g. “Biomedical Laboratory”), Driver (e.g. “Develop innovative products”), Goal (e.g. “Confidentiality of Personal Information”), Principle (e.g. “European Personal Data Privacy Directive”), Requirement (e.g. “Access control on biomedical analysis prescription”) and Assessment (e.g. “Risk of disclosure of personal data due to lack of employee’s awareness”).

Thus, the desire for a laboratory to develop home care services can be expressed using a Goal (“Develop biomedical

homecare Services”) which is based on the willingness for a laboratory to develop innovative services (Driver “Develop innovative products”) while taking into account the growing demand for home care services (Driver “Increased demand for home care”) by patients (Stakeholder “Patient”).

Another aspect related to the Motivation view is the fact that to handle biomedical analysis prescriptions (which are medical data, so sensitive data) (Requirement “Access control on biomedical analysis prescription”) as well as legislation (Principle “European Personal Data Privacy Directive”) require confidentiality. This need for confidentiality can therefore be expressed as a Goal (“Confidentiality of Personal Information”). Both Principle and Goal can then be seen as a Driver (“Confidentiality”) that is associated with the Stakeholder “Privacy Regulator”, responsible for ensuring that the laboratory complies with the legislation. Last but not least, an Assessment “Risk of disclosure of personal data

Table 1 ArchiMate—ISSRM concepts alignment table


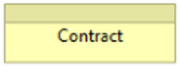
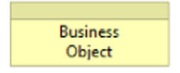
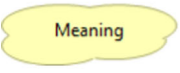

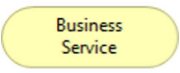
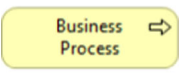
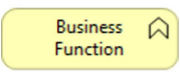
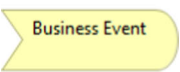
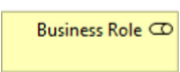
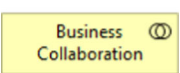
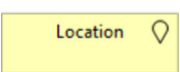
ArchiMate 2.1	ISSRM domain model	ArchiMate 2.1 concept <Semantic mapping type> ISSRM concept	Running example
<i>Business Layer</i>			
	Business asset::value	<i>equivalence</i>	“Home care”
	Business asset	<i>specialisation</i>	“Home Blood Analysis”
	Business asset	<i>specialisation</i>	“Contract”
	Asset	<i>specialisation</i>	“Biomedical Analysis Prescription”
	Business asset	<i>specialisation</i>	“Prescribed Analyses”
	IS asset	<i>specialisation</i>	“Biomedical Paper Prescription”
	Business asset	<i>specialisation</i>	“Home Blood Taking”
	Business asset	<i>specialisation</i>	“Take Blood Home”
	Business asset	<i>specialisation</i>	“BioMedical PreAnalysis”
	Business asset	<i>specialisation</i>	n/a
	n/a	<i>n/a</i>	n/a
	IS asset	<i>specialisation</i>	“Home Analysis Call Center”
	Business asset	<i>specialisation</i>	“Nurse”
	Business asset	<i>specialisation</i>	n/a
	IS asset	<i>specialisation</i>	“Patient Home”
	IS asset	<i>specialisation</i>	“An independent nurse”

Table 1 continued

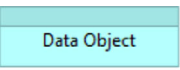

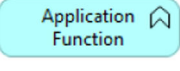
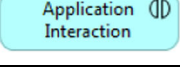
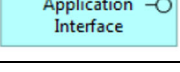
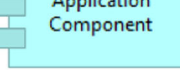



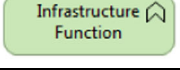
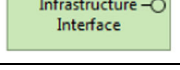
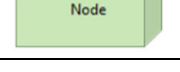
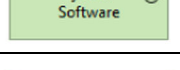
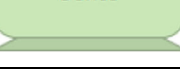
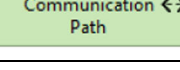
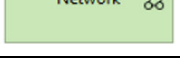
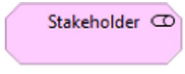
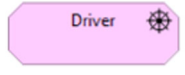
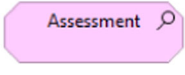

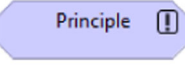
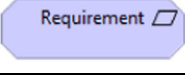
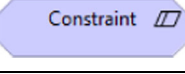
<i>Application Layer</i>			
	IS asset	<i>specialisation</i>	“Biomedical Prescription Data”
	IS asset	<i>specialisation</i>	“Prescription Input”
	IS asset	<i>specialisation</i>	“Prescription Management”
	IS asset	<i>specialisation</i>	n/a
	IS asset	<i>specialisation</i>	“Mobile Prescription Management”
	IS asset	<i>specialisation</i>	“Prescription Mobile App”
	IS asset	<i>specialisation</i>	n/a
<i>Technology Layer</i>			
	IS asset	<i>specialisation</i>	“Prescription Mobile Application”
	IS asset	<i>specialisation</i>	n/a
	IS asset	<i>specialisation</i>	n/a
	IS asset	<i>specialisation</i>	n/a
	IS asset	<i>specialisation</i>	“Mobile Node”
	IS asset	<i>specialisation</i>	“Mobile OS”
	IS asset	<i>specialisation</i>	“Tablet”
	IS asset	<i>specialisation</i>	n/a
	IS asset	<i>specialisation</i>	“WiFi”

Table 1 continued

<i>Motivation Extension</i>			
 Stakeholder	Asset	<i>association</i>	“Privacy Regulator”
 Driver	Security criterion	<i>generalisation</i>	“Confidentiality”
 Assessment	Risk	<i>generalisation</i>	“Risk of disclosure of personal data due to lack of employee’s awareness”
 Goal	Security objective	<i>generalisation</i>	“Confidentiality of Personal Information”
 Principle	Asset	<i>association</i>	“European Personal Data Privacy Directive”
 Requirement	Security requirement	<i>generalisation</i>	“Access control on biomedical analysis prescription”
 Constraint	Security requirement	<i>generalisation</i>	n/a

- As established in the alignment table, most of the core concepts of the Business Layer of ArchiMate are specific kinds of business assets.
- There is (only) one ArchiMate concept that is mapped to a metric of ISSRM domain model: *Value* that is equivalent to the value of a business asset [37].
- All of the ArchiMate concepts of the Application and Technology Layers 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. This alignment is compliant with the definition provided by the ArchiMate specification [20] (“*The Application Layer supports the Business Layer with application services which are realised by (software) applications. The Technology Layer offers infrastructure services (e.g. processing, storage, and communication services) needed to run applications, realized by computer and communication hardware and system software.*”)
- Application and Technology Layers 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, both classes can be represented with the help of the following concepts of the Business Layer: *Location* and *Business Actor*. *Location* and *Business Actor* are thus considered as specialisations of IS asset. For a “pure” IT-based process, the Business Layer is used to represent the business assets and the Application and Technology Layers the IS assets. For a non-IT process, only the Business Layer is used to represent both the business and IS assets. In the general case, the IS assets are represented by a mix between business (people, facilities) and application and technology elements (hardware, software, network).
- We treat *Business Role* (e.g. mechanical engineer, CFO) as a specialisation of business asset and *Business Actor* (e.g. John Doe) as a specialisation of IS asset. The *Business Role* is indeed the business aspect of a person involved in the enterprise, but the *Business Actor* is the physical/material representation of this person, thus potentially the target of threats (e.g. social engineering, theft of material) or source of specific vulnerabilities (e.g. lack of awareness, inadequate recruitment procedures, incorrect use of software), that are both characteristics of IS assets.
- The concept of *Business Object* is a specialisation of the concept of asset (i.e. it can be used to represent a business asset or an IS asset). When going further in a *Business Object* specification, *Meaning* related to a *Business Object* is the “business side” of an asset as defined in the ISSRM domain model (the focus is on the knowledge or expertise, i.e. the informational payload of the asset), and *Representation* the “IS side” of this asset: the perceptible (or material) form of the information (e.g. sheet of paper on which is written the information). In line with the preceding finding, this specialisation is only relevant in the frame of “paper-based” information systems. In the other case, it is not the concept of *Representation* that

is used to represent the “IS side” of the business objects, but concepts from the Application or Technology Layer such as, basically, *Data Object*.

- *Business Event* has no mapping to any ISSRM concept. It is defined as something that happens (internally or externally) and influences behaviour. It is thus the trigger of a *Business 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 catching behavioural and methodological aspects of ISSRM.
- *Structure Element* and *Motivational Element* do not have any mapping to ISSRM concepts and are not of interest here, because they are abstract entities that are not instantiated [20].
- *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). Regarding our scope, the changes in an organisation are created, motivated, and fuelled by the need of confidentiality, integrity, or availability of information processed in the IS. In the same vein, the concept of *Goal* is a generalisation of security objective. In our scope that is ISSRM, the end state that a stakeholder intends to achieve is confidentiality, integrity and/or availability of business assets.
- *Assessment* is considered as a generalisation of risk, because a risk is a specific kind of assessment. A risk is indeed the end result of some analysis of some *Driver* (i.e. confidentiality, integrity, and/or availability).²
- *Requirement* is a generalisation of security requirement. The same applies for *Constraint* that is a specific kind of *Requirement* in ArchiMate: *Constraint* is related to *Requirement* by a “IS A” relation in the ArchiMate meta-model.
- The concepts of *Stakeholder* and *Principle* are associated with the concept of Asset. *Stakeholder* (e.g. regulation organisation, customers, shareholders) and *Principle* (e.g. standard to be followed, regulation) are indeed used in ArchiMate to represent aspects considered as part of the environment of the assets and identified during the context establishment step of the ISSRM process [8]. Concepts currently composing the ISSRM domain model are the set of concepts used during risk assessment and risk treatment steps.

To summarise, we can draw two main conclusions from our alignment table. First, although the mapping is complex, EAM brings a more fine grained representation of (business and IS) assets. Second, EAM considers concepts that are

part of the environment of assets. This is not the case of the ISSRM domain model.

6 EAM-ISSRM integrated model proposal

As indicated above, we have analysed the three other references selected (TOGAF, DoDAF and IAF) in the same manner as what we have performed in the preceding section for ArchiMate [34,35]. Then, for each reference analysed, we have built a TOGAF-, DoDAF-, and IAF-specific EAM-ISSRM integrated model. In this section, we integrate these four method-specific EAM-ISSRM integrated models into an overall integrated EAM-ISSRM model.

Our context is ISSRM, and the EAM-ISSRM integrated model shall be suited to this context. As a consequence, in the ArchiMate-, TOGAF-, DoDAF- and IAF-ISSRM integrated models, the EAM concepts that generalise an ISSRM concept (see Table 1) will be dropped in the integrated model, because they are too generic for our purpose. On the other hand, EAM concepts having relations of other kind (for example: specialisation, association) are of particular interest for consideration in the EAM-ISSRM integrated model.

In our design group, we have agreed on two ways of improving the ISSRM domain model with EAM aspects: the introduction of the environment of the assets and the refinement of business and IS assets. The conclusions drawn from the alignment tables of the three other EAM references are indeed aligned with the ones of those drawn for ArchiMate [34]. The resulting EAM-ISSRM integrated model is shown in Fig. 6, where extensions of the ISSRM model are shown in black with white labels. The following subsections report on how this model was constructed.

Finally, our work is focused on the so-called concepts of ArchiMate, and not on the relationships between these concepts. It is theoretically possible to define the same kind of alignment table for relationships between concepts, as it has been done for concepts in Sect. 5. However, our attempt to do so for the ISSRM domain model [7,38] made clear that this generates a huge set of relationships that does not clarify much, as all of the required information can already be found in the definitions of the concepts that are already available. Thus, based on the concept definitions of the different studied references, every newly introduced concept is analysed to see if it is linked (and how) with other concepts. The multiplicities of the relations between the concepts are defined too. This analysis is done iteratively, for each source of the selected literature, and a consensus is found within the design group for each introduced relationship.

² *Assessment* is defined in ArchiMate as the outcome of some analysis of some driver [20].

Fig. 6). By analogy with the definition of environment of a system³ in ISO/IEC/IEEE 42010:2011 [25], *Constraint* is defined as developmental, technological, business, operational, organisational, political, economic, legal, regulatory, ecological and social norms that can affect the assets. The ISO/IEC 27005:2011 definition of *Stakeholder* is adopted: person or organisation that can affect, be affected by, or perceive themselves to be affected by a decision or activity [8]. These definitions are deliberately not extracted from a specific EAM reference and are generic enough to be adapted to the various EAM references studied. To be specific:

ArchiMate: Principle can be used to represent *Constraint*, and *Stakeholder* can be used to represent *Stakeholder*;

TOGAF: *Constraint*, *Assumption* and *Principle* can be used to represent *Constraint*, and *Role* and *Organisation unit* can be used to represent *Stakeholder*;

DoDAF: *Condition*, *Guidance*, *Rule*, *Agreement* and *Standard* can all be used to represent *Constraint*.

6.2 Introduction of different kinds of business and IS assets

In the ISSRM domain model, the assets are classified as Business assets or IS assets. This makes it impossible to model the complexity of current targets of assessment. We need to refine the ISSRM model here, and the four analysed EAM languages provide examples of how to do this. They contain the following classes of assets:

- *ArchiMate*: Business Layer, Application Layer, and Technology Layer
- *TOGAF*: Business architecture, Data architecture, Application architecture (the two latter being grouped in IS architecture in some overviews of the TOGAF meta-model), and Technology architecture
- *IAF*: Business architecture, Information architecture (both of them being instances of business assets), IS architecture, and Technology architecture
- *DoDAF* does not provide in its conceptual model such layers/architecture classes

ISO/IEC 27005:2011 lists the following business assets (also called “primary assets”):

- Business processes & activities
- Information

and the following IS assets (also called “supporting assets”):

- Hardware
- Software
- Network
- Personnel
- Site
- Organisation’s structure

The design group stated that a *Business element* class, excluding site, personnel and organisation aspects, is an instance of *Business asset*. Moreover, an *Application element* class, a *Technology element* class, a *Location* class, an *Actor* class and an *Organisation* class are instances of IS assets. With such a proposal, we are compliant with the definitions provided in the ISSRM domain model, and we also fully cover the taxonomy provided in ISO/IEC 27005:2011. Finally, it is also necessary to add first a reflexive relation on business asset, and second a reflexive relation on IS asset. These two relations make clear that, with an EAM support to ISSRM, it is now possible to highlight the links existing between business assets and those between IS assets. Such kind of links helps to deal with IS complexity, enterprise evolution, and documentation improvement for ISSRM activities. The resulting extension is presented in Fig. 6.

7 EAM-ISSRM integrated model validation

Following the definition proposed by Wynekoop and Russo [39], evaluation of a conceptual model is defined as the systematic study of the conceptual model to determine its usefulness, effect or impact. Regarding our research agenda [13], we first want to demonstrate the usefulness of our model as the conceptual foundation to design a framework (modelling language, method, and tool) to perform ISSRM. Based on the survey of ontology evaluation techniques provided by Brank et al., we decided to go for a combination of assessment by humans with application-based evaluation [40], that are the suited approaches when no “golden standard” and no relevant source of data about the domain (e.g. collection of documents—these have already been used for the design of the model) are available to be compared with the evaluated model. Considering the classification provided by Recker [41], this approach is an empirical evaluation: more specifically a combination of a survey (use of questionnaire to gather human attitudes, opinions, and impressions) with a case study (systematic observation of a particular group or subject that utilises the investigated artefact). The research design established is described in the next section. The results obtained with the validation group come after, and finally the conclusions from results as well as threats to validity are discussed.

³ “The environment of a system includes developmental, technological, business, operational, organisational, political, economic, legal, regulatory, ecological and social influences” [25].

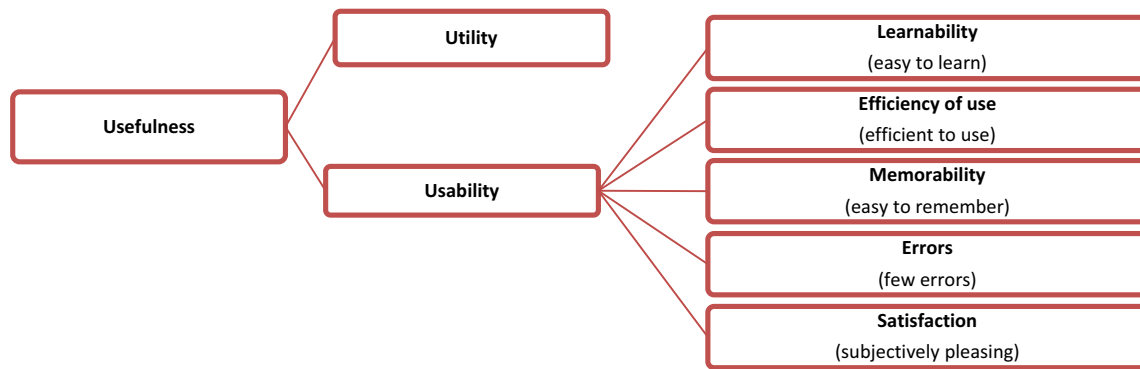


Fig. 7 Usefulness decomposition

7.1 Experiment design for the EAM-ISSRM integrated model validation

In order to validate the EAM-ISSRM integrated model, we want to answer the following research question: is the EAM extension of the ISSRM domain model, namely the EAM-ISSRM integrated model, useful, i.e. utile and usable? More specifically, we want to collect information about its utility to deal with the challenges identified in the introduction (i.e. enterprise complexity and continuous evolution, regulatory pressure, and weakness of the documentation) and its usability as the conceptual foundation to design our framework to perform ISSRM. To do so, we have elaborated a validation method for the EAM-ISSRM integrated model, based on a validation group composed of experienced ISSRM practitioners, who have answered questions and performed exercises (see Appendixes).

7.1.1 Conceptual framework

Our objective is to test the usefulness of the EAM-ISSRM integrated model as the conceptual foundation to design a framework (modelling language, method, and tool) to perform ISSRM. To do so, we use the criteria of utility and usability, based on Nielsen's definition [42] (see Fig. 7). These criteria have been used for years in different contexts, especially for validating security-related artefacts [43]. We assess the usefulness of the EAM-ISSRM integrated model through questions and exercises, and through the satisfaction to use a system based on this model with the help of a SUS (System Usability Scale) questionnaire [44]. Created in 1996, SUS has become an industry standard, with references in over 3000 articles and publications. According to the literature [45], SUS generally requires at least 12 subjects to produce "correct" conclusions (100% accurate), but already provides 75% accuracy starting from eight subjects and thus is appropriate for a small sample of subjects as in this experimentation.

The following definitions, inspired by the work of Nielsen [42] are adopted for "utility", "usability", and its subcomponents.

Utility demonstrates if the model provides the features that are necessary for its purpose. We operationalize it as whether the EAM-ISSRM integrated model can be used in practice by the validation group members, as well as their feedback on how supportive it is to deal with the identified challenges, i.e. to manage enterprise complexity and continuous evolution, deal with regulations, and improve resulting documentation compared to the ISSRM domain model.

Usability allows showing how easy and pleasant these features are to use. Usability can be defined by 5 quality components, namely learnability, efficiency, memorability, errors, and satisfaction. We operationalize them in the following way [42]:

- *Learnability*: "The [model] should be easy to learn so that the user can rapidly start getting some work done with the [model] ", "Capability of a [model] to enable the user to learn how to use it" or "How easy is it for users to use the [model] the first time they encounter it".
- *Efficiency of use*: "The [model] should be efficient to use, so that once the user has learned the [model], a high level of productivity is possible", "Resources spent by user in order to ensure accurate and complete achievement of the goals" or "Once users have learned the [model] , how quickly can they perform tasks".
- *Memorability*: "The [model] should be easy to remember, so that the casual user is able to return to the [model] after some period of not having used it, without having to learn everything all over again", "Quality of a [model] of being easy to remember or worth remembering" or "How well the [model] allows people to remember how to do things".
- *Errors*: "The [model] should have a low rate, so that users make few errors during the use of the [model] , and so that if they make errors they can easily recover

from them”, “How well the [model] prevents errors and allows recovery from them”.

- Satisfaction: “The [model] should be pleasant to use, so that users are subjectively satisfied when using it, they like it”, “The extent to which the [model] is pleasant to use” or “How satisfied a user is with the [model]”.

7.1.2 Meeting design and preparation

A validation group was established and composed of experienced ISSRM practitioners. We considered including EAM experts in the validation group, but we decided not to do so because our goal is to improve ISSRM and our target of users is focussed on ISSRM practitioners. As a consequence, in order to perform the experimental tasks, the validation group members should have an ISSRM background. In addition, because our validation group will use the concepts of the ISSRM domain model, to have a good knowledge of these concepts is necessary. Indeed, as described below in the structure of the validation group meeting, the validation is focused on the evolution to the EAM-ISSRM integrated model, the ISSRM domain model as such having already been validated in our previous work [7]. As selection criteria, we decided thus that validation group members should have a practical experience with the tool we developed for the ISSRM domain model, called TISRIM [46,47].

The users of TISRIM have been contacted personally (email and/or phone call) to ask them about their interest to be part of the validation group. Only people who were not involved in the design stage of the EAM-ISSRM integrated conceptual model were eligible.

The structure of the validation group meeting was as follows:

- a) Introduction: General introduction to the topic and the objectives of the meeting. Reminder about the concepts of the ISSRM domain model. (40 min.)
- b) Pretest survey (see Appendix 1): Open question about the strengths and the weaknesses in performing ISSRM based on TISRIM and the ISSRM domain model. (20 min.)
- c) Execution: After having exposed the EAM extension for the ISSRM domain model (30 min.), the participants need to perform two exercises and fill one questionnaire (see Appendix 2):
 - Exercise 1: Based on the description of a case, members of the validation group need to identify an instance of each concept of the EAM-ISSRM integrated model [specifically helps to assess learnability and errors]. (40 min.)

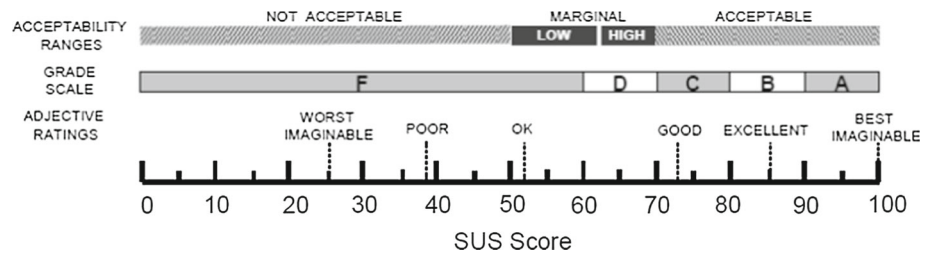
- Exercise 2: Based on the requirements provided in ISO/IEC 27001 [6], members of the validation group need to identify if, by instantiating the EAM-ISSRM integrated model, and more specifically its extension, some requirements are satisfied and which ones [specifically helps to assess utility and errors]. (20 min.)
- SUS questionnaire [44] about usability of the EAM-ISSRM integrated model. (10 min.)

- d) Post-test survey (Appendix 3): Ask people to recap about the concepts that are part of the EAM extension of the ISSRM domain model [specifically helps to assess memorability]. (15 min.)
- e) Closure: Ask people about their general feedback about the potential felt that the EAM-ISSRM integrated model is suitable as the conceptual foundation to design a framework to perform ISSRM [specifically helps to assess utility and satisfaction]. (30 min.)

Before the actual validation group meetings, a trial of the material and of the approach was performed with three members of our research group (they were not involved in the design of the EAM-ISSRM integrated model). The objective was to detect and correct errors in the material, improve the presentation of the EAM-ISSRM integrated model and of the different exercises, and finally test the feasibility of completing the exercises in the available time. Based on this trial, the following changes have been made to the material:

- In *exercise 1*, only one instance per concept (instead of two) was asked to reduce the risk of non-completion of the exercise within the allotted timeslot, since one instance seems enough to show if a subject understands or not a concept;
- In *exercise 2*, two different placeholders were added, in order to specifically collect requirements covered by the ISSRM domain, and those covered by the EAM extension;
- In *post-test survey*, subjects are now asked to recap not only the concepts from the EAM extension, but also their linked concepts in the ISSRM domain model. This in order to verify that subjects have not only memorised the EAM extension concepts, but also how they are integrated with the ISSRM domain.
- Some rephrasing of the items of the *SUS questionnaire* were done to better highlight the prospective aspect of the questionnaire (the questionnaire asks not about the EAM-ISSRM integrated model itself, but about an ISSRM tool that would be based on this model).

Fig. 8 A comparison of the adjective ratings, acceptability scores, and school grading scales in relation to the average SUS score [50]



7.1.3 Variable measurements and their interpretation

Through the various exercises carried out by the participants, the different components of usefulness, namely utility and usability, will be estimated as follows.

With regard to *Utility*, measurement is twofold: (1) the ability of the subjects to perform a given task in which the use of the model is necessary (i.e. exercises 1 and 2) shows whether the model is instantiable within the defined framework and understood by the subjects, and (2) the potential felt by subjects after using the EAM-ISSRM integrated model shows if its use demonstrates some advantages compared to traditional approaches. Thus, in practice, (1) is estimated both by the time required by participants to complete exercises 1 and 2 as well as by the error rate of exercises 1 and 2 (i.e. the ratio of the number of errors compared to the number of correct responses), while the general feedback of subjects on the EAM extension collected during closure is used to estimate (2).

Concerning *Usability*, in accordance with Nielsen [42], the different components will be measured as follows:

Satisfaction is measured based on the answers provided to the SUS questionnaire (see Appendix 2), composed of 10 items that participants must answer using a Likert scale (five response options—from *Strongly agree* to *Strongly disagree*). Inasmuch as the final purpose of the model is not to be directly manipulated by subjects (they will rather use a tool based on this model), measuring satisfaction of using the model seems not the most relevant measure. Therefore, the questionnaire asks not about the EAM-ISSRM integrated model itself, but about an ISSRM tool that would be based on this model. Subjects' scores for each question are combined to obtain a score comprised between 0 and 100. Such a score is then compared to a standard distribution of SUS scores [48,49], i.e. the mean value being around 68. To allow a better interpretation of this global score, the scale presented in Fig. 8 shows how the latter can be qualified in terms of acceptability range (from *Not acceptable* to *Acceptable*), Grade scale (from *F* to *A*) and adjective ratings (from *Worst imaginable* to *Best imaginable*) is used [50].

Learnability is measured, on the one hand, by ensuring that subjects are able to complete exercises 1 and 2 in the allotted time (respectively 40 and 20 minutes). In other words, being able to complete the exercises in the allotted time allows

estimating the ease of learning and mastery of concepts the first time subjects are faced with these concepts. These durations have been set in advance and confirmed during the trial, based on the proposition that if people from our research group (not involved in the design of the EAM-ISSRM integrated model, but meeting the necessary inclusion criteria) succeed to complete the exercises in time, regular subjects should also be able to succeed. In addition, the answers to items 4 (*I think that I would need the support of an expert to be able to use such a system*) and 10 (*I would need to learn a lot of things before I could get going with such a system*) of the SUS questionnaire (see Appendix 2), combined together as a sub-score, are also used to estimate *Learnability*.

Efficiency has been set aside, because this can only be measured once a method and a tool are defined. Measuring the efficiency of our approach is part of our future work.

Memorability is estimated using the restitution rate of the post-test survey (i.e. the ratio of the number of correct listed concepts compared to the number of expected concepts). Restitution rate should be as high as possible. In parallel, the lowest returned concepts provide insight on their own memorability. Ideally, we should have asked subjects to do similar exercises some days later, relying on their memory of the model. Unfortunately, this was not possible given the busy schedules of our subjects. So we subjected them to a memory test at the very end of the session, making the assumption that the results of the test performed a few hours later does give some information about memorability.

Errors are estimated using the total number of errors made in exercises 1 and 2. Minor and major errors are distinguished—a *major error* is defined as an error suggesting that the user did not understand the general meaning of the concept (confusion with another concept, no link can be established between the user's response and the concept in question), while a *minor error* is defined as a misinterpretation of the example, but suggesting that the user has understood the general meaning of the concept. Of course, the number of (minor and major) errors should be as low as possible. In addition, we used the number of errors made per concept to identify the concepts of which the definition had to be improved.

Table 2 Participants' profile

#	Sector	Position	Experience (years)
1	Telecommunications	Information Security Officer	1
2	Data centres, Cloud services	Chief Information Security Officer	15
3	Data centres, Cloud services	Security consultant & Deputy Chief Information Security Officer	8
4	Public research centre	System administrator	15
5	Telecommunications	Information Security Officer	8
6	European and international institutions	Chief Information Security Officer & Data Protection Officer	23
7	Public research centre	Network engineer	19
8	Archiving, Cloud services, Data centre	Information Security and Risk Manager	3
9	Corporate services	IT Manager & Chief Information Security Officer	10

7.2 Results

The results of the validation are depicted first by detailing meeting attendance and duration of the validation group, then, the measures of variables are reported.

7.2.1 Meeting attendance and duration

Based on our inclusion criteria for members of the validation group, 13 potential participants were contacted. Nine of them accepted, three declined because of lack of availability, and one did not provide any answer to our request. Two different sessions were organised to deal with schedule constraints of the participants: the first one with 7 participants and the second one with 2 participants. The total length of each session was 3 hours. The profile of the participants in terms of position and experience is detailed in Table 2.

7.2.2 Variable measurement through the exercises performed by the validation group

With regard to *Utility*, all the participants were able to complete the two exercises within the expected time and even below (median times: 39:00 for exercise 1 and 14:16 for exercise 2), while the error rate is globally low with a median error rate of 12.50% (standard deviation (SD) of 0.13, mean of 15.28%) for exercise 1 and a median error rate of 0.00% (SD of 0.29, mean of 16.67%) for exercise 2. The graph in Fig. 9 shows the time spent by participant with regard to error rate for exercises 1 and 2. There are two extreme cases, namely User#9 who spent much time on exercise 2 for a high error rate (83.33%), and User#5 who ended the exercise 2 quickly (8:26) without any error. Other than these two extreme cases, the distribution time-error rate is homogeneous.

Besides experimentation through exercises, participants' general feedback helps to get an idea about their perception of the utility and usefulness of our new model. The following advantages for the EAM-ISSRM integrated model compared to traditional approaches represented by the use of TISRIM, which is based on the ISSRM domain model, were mentioned:

- a greater degree of contextualisation,
- a better understanding of the scope,
- an easier maintainability of the risk management results over time, and
- a better compliance thanks to a broader scope of study.

On the other hand, some participants point out that such a model will increase the risk management effort.

In addition, some people mentioned that some concepts (especially *Actor* and *Organisation*) would benefit from a better definition to understand the relationship and difference between them.

Concerning *Usability*, the median measured SUS score is equal to 75 with a SD of 12.53 (mean equal to 72.78). Compared to the scale provided by Bangor et al. [50] and presented in Fig. 8, such score, graded as C on a scale from A to F (A being the best and F the worst), is considered as “good”, and corresponds in terms of acceptability to an “acceptable” artefact (the best acceptability range, as described in Fig. 8).

Concerning *Learnability*, all the participants managed to complete the two exercises within the timeframe (median time of 39 minutes with a SD of 3:53 (mean equal to 37:10) for exercise 1 and a median time of 14:16 with a SD of 2:59 (mean equal to 13:50) for exercise 2).

On the other hand, the median sub-score obtained for items 4 and 10 of the SUS questionnaire is equal to 75 with a SD of 18.75 (mean equal to 75). These items ask whether the

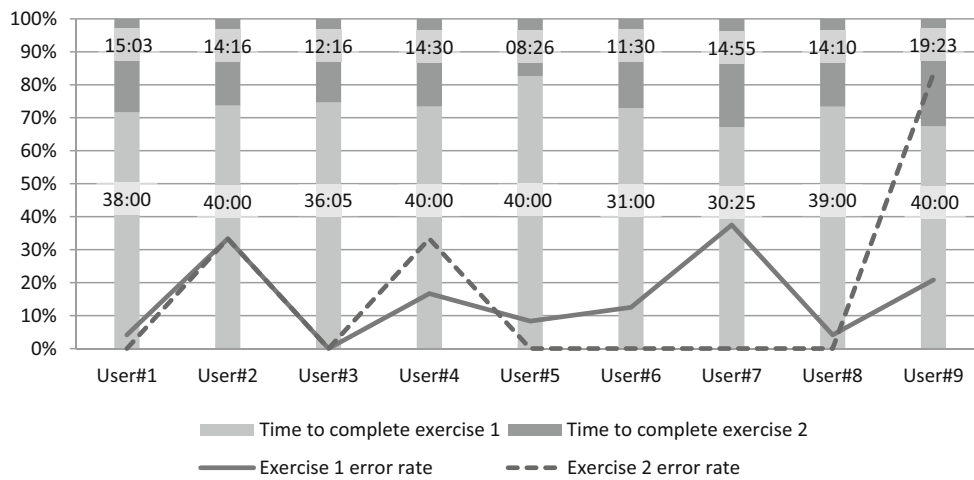
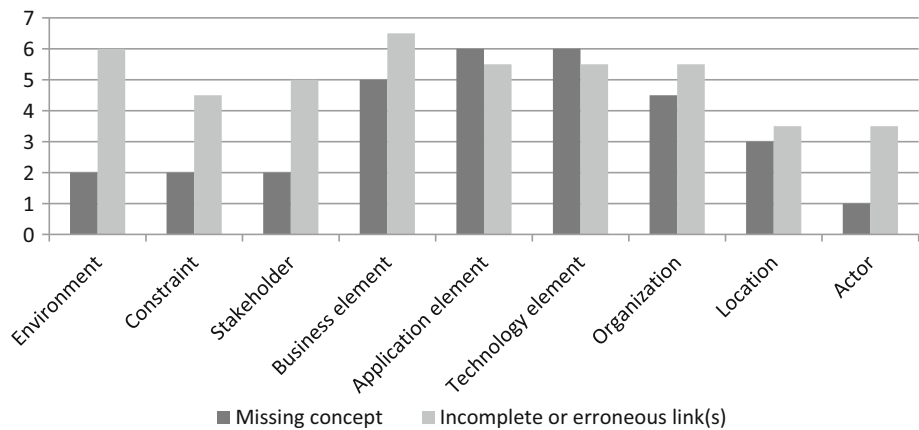


Fig. 9 Time spent and error rate for exercises 1 and 2

Fig. 10 Errors made in concepts' restitution



subject thinks he or she needs the support of an expert to be able to use a system that supports the integrated EAM-ISSRM model (item 4), and whether the subjects expect to have to learn a lot before he or she could use the system (item 10). Compared to the scale presented in Fig. 8, such a score is graded as C on the scale from A to F and corresponds in terms of acceptability to an “*acceptable*” artefact for learnability aspects.

Concerning *Memorability*, the median restitution rate is equal to 58.33% with a SD of 0.36 (mean equal to 52.47%). Concepts that cause the most problems in terms of restitution (both for the concept itself and for its links within the model) are *Business element*, *Application element* and *Technology element*, as depicted in Fig. 10. Moreover, the relations of the concept *Environment* are not very well remembered.

With regard to *Errors* made during exercise 1, in which participants were asked to identify 24 concepts (15 from ISSRM and 9 from EAM), the number of errors is shown in Table 3.

These results show an error rate for minor errors almost identical for both ISSRM and EAM parts (around 11%), but

a slightly higher error rate for major errors for the EAM part (18.52%) compared to the ISSRM part (13.33%). In order to refine these results, in a second step, we compared the errors on the EAM part of the model to the number of errors committed in the ISSRM part. Our assumption is that subjects having committed more than one-third of errors on the ISSRM concepts of the integrated model do not master the initial model, which was a prerequisite for being part of the validation group (*wrt* the inclusion criteria). Thus, Table 4 shows errors distribution of exercise 1 excluding the two subjects who do not master the ISSRM concepts.

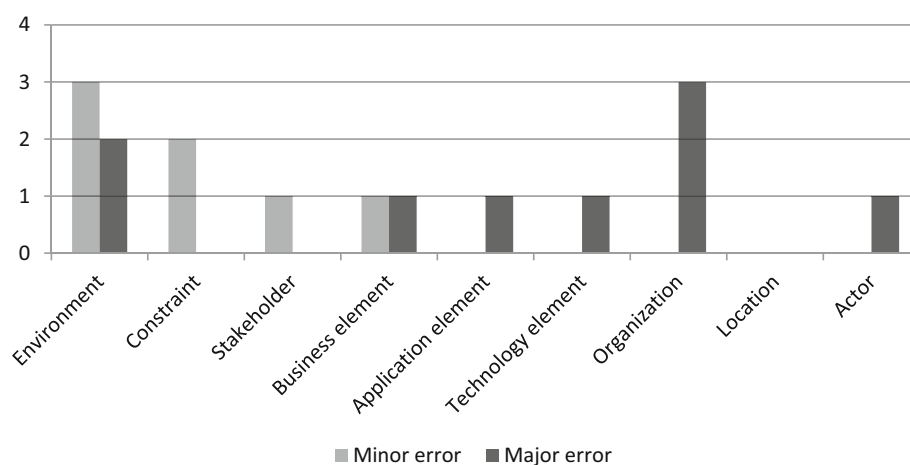
These revised figures show that a good mastery of the ISSRM model implies a better mastery of the EAM-ISSRM integrated model (especially in terms of major errors) for these subjects. Indeed, by excluding subjects with limited mastery of the ISSRM part, the median major errors rate falls from 12.50 to 8.33% while the average major errors rate falls from 15.28 to 9.52%. Meanwhile, the minor errors rates remain more or less stable (median 8.33%, mean 11.57 to 11.90%). To go further, Fig. 11 shows the distribution of errors by concepts for the most error-prone concepts. The

Table 3 Exercise 1 errors distribution

		Minor errors			Major errors		
		Median	SD	Mean	Median	SD	Mean
ISSRM	Number of errors	2.00	1.20	1.78	1.00	2.12	2.00
	Error rate	13.33%	–	11.85%	6.67%	–	13.33%
EAM	Number of errors	0.00	1.22	1.00	1.00	1.32	1.67
	Error rate	0.00%	–	11.11%	11.11%	–	18.52%
ISSRM-EAM	Number of errors	2.00	1.72	2.78	3.00	3.16	3.67
	Error rate	8.33%	–	11.57%	12.50%	–	15.28%

Table 4 Exercise 1 errors distribution (excluding the two subjects who do not master the ISSRM part)

		Minor errors			Major errors		
		Median	SD	Mean	Median	SD	Mean
ISSRM	Number of errors	2.00 (→)	1.35 (↗)	1.86 (↗)	1.00 (→)	0.82 (↘)	1.00 (↘)
	Error rate	13.33% (→)	–	12.38% (↗)	6.67% (→)	–	6.67% (↘)
EAM	Number of errors	0.00 (→)	1.29 (↗)	1.00 (→)	1.00 (→)	1.25 (↘)	1.29 (↘)
	Error rate	0.00% (→)	–	11.11% (→)	11.11% (→)	–	14.29% (↘)
ISSRM-EAM	Number of errors	2.00 (→)	1.95 (↗)	2.86 (↗)	2.00 (↘)	1.80 (↘)	2.29 (↘)
	Error rate	8.33% (→)	–	11.90% (↗)	8.33% (↘)	–	9.52% (↘)

Fig. 11 Errors distribution by concepts

distribution shows that the concepts *Organisation* and *Environment* are the less well understood by the participants.

During exercise 2, six main responses were expected; the numbers of errors for exercise 2 are shown in Table 5. The error rate for minor errors is high; indeed some participants provided a large number of answers, including incorrect answers. Each individual wrong answer was then considered as a minor error. Thus, for a same expected response, more than one minor error can be considered.

7.3 Discussion of the results and threats to validity

In this section, we first draw conclusions regarding utility and usability of the model, including improvement opportunities, and then discuss some threats to validity we identified.

7.3.1 Results summary and conclusions

The objective of the validation group meetings was to evaluate the utility and usability of the EAM-ISSRM integrated model. Based on the results obtained, we conclude that the participants found the model useful. The fact that the distribution time-error rate is homogeneous suggests that for most subjects, the model as defined is instantiable within the defined framework (spent time) and is understood (error rate). The results also indicate that concepts are sufficiently explicit to allow rapid learning and mastery (see *Learnability*). The two extreme cases, that we have decided to exclude, indicate that for individual cases, using the model may be too difficult or at the opposite very easy (see *Utility*). The EAM part seems more difficult to master for the subjects,

Table 5 Exercise 2 errors distribution

	Minor errors			Major errors		
	Median	SD	Mean	Median	SD	Mean
Number of errors	3.00	7.50	5.78	0.00	1.73	1.00
Error rate	50%	–	96.33%	0.00%	–	16.67%

which makes sense, since subjects were selected to be familiar with the concepts of the ISSRM part (see *Errors*). The model has been assessed by the subjects as being good and having the best acceptability range on the used scale (see *Usability*). Combining these results with the low rate of major errors in exercises, and with the self-perception that the subjects would need expert help to get going with the integrated model, we conclude that the overall EAM-ISSRM integrated model is well understood by the participants but that expert support should be provided to adopt it in routine practice.

A set of advantages of the EAM-ISSRM integrated model compared to traditional approaches were highlighted by the subjects (see *Utility*):

- a greater degree of contextualisation,
- a better understanding of the scope,
- an easier maintainability of the risk management results over time,

all of them contributing to the mitigation of challenges 1, 2 and 4, namely complexity of current IS and increasing number of threats, continuous evolution of organisations, and difficulty to have a clear and manageable documentation for ISSRM activities, and

- a better compliance thanks to a broader scope of study,

contributing to the mitigation of challenge 3 about regulatory pressure on organisations involving ISSRM requirements.

The subjects as well as their results of the exercises highlighted also some necessary improvements:

- Some people mentioned that *Actor* and *Organisation* would benefit from a better definition to understand the relationship and difference between them. Moreover, the concepts *Organisation* and *Environment* seem not well understood by the participants when analysing the results of exercise 1. As a consequence, we modified the definition of *Organisation*, making clear that an organisation may include actors (see *Utility* and *Errors*).
- Although they were well understood (see *Errors*), concepts that cause the most problems in terms of restitution (both for the concept itself and for its links within the model) were *Business element*, *Application*

element and *Technology element* (see *Memorability*). Combined with the observation that the overall EAM-ISSRM integrated model is well understood by the participants but that expert support should be provided to adopt it in routine practice, we concluded that additional efforts shall be done by experts when presenting and explaining *Business element*, *Application element* and *Technology element* to facilitate their adoption by users.

- The relations of the concept *Environment* appear also not to be very well understood and remembered (see *Memorability* and *Errors*). As a consequence, improvements of the model and of the related definitions have been discussed and integrated in our current version of the EAM-ISSRM integrated model: a better definition of *Environment*, making clear its relation with the other concepts, combined with a necessary additional effort to explain this concept.

Last but not least, the fact that some users point out that such a model will increase the risk management effort compared to the original ISSRM domain model is obvious, since the integrated model includes additional concepts to be considered in risk management. However, this effort is in a way unavoidable because these concepts are required for compliance purpose, although to take them into account in a systematic, formal and complete way requires an additional work. The method and tool support to be provided for the integrated model can try to minimise this additional effort, but it cannot eliminate it.

7.3.2 Threats to validity

In order to ensure the validity of the results and conclusions presented above, it is important to list the identified threats to validity and the associated rationale and mitigation measures in place.

First, the validation group members selection criteria (“*validation group members should have a practical experience with the tool that we have developed for the ISSRM domain model, called TISRIM*”) involve a small sample, since the user base is composed of 16 people (3 of them being abroad and thus not contacted for logistics reasons). A larger population could have been better to increase the external

validity of the results. Due to our selection criteria, the participants will be representative of the intended population of security risk management practitioners that are familiar with the state-of-the-art concepts of ISSRM, as described in the ISSRM domain model, but not for the bigger population of security risk management practitioners, including those currently working with concept-specific methods. The most we can claim for this bigger population is that if they would become familiar with the state-of-the-art ISSRM concepts, it is reasonable to expect that they would behave similarly to our validation group, although of course we cannot predict this with absolute certainty, and neither can we quantify our uncertainty.

Still regarding subjects, the validation group members selection criteria itself (subjects familiar with both the ISSRM domain model and the TISRIM) implies a limited external validity, as we cannot claim it would achieve the same results with subjects unfamiliar with the ISSRM domain model nor with TISRIM. To support such a claim, future research should validate the integrated model with ISSRM professionals unfamiliar with the ISSRM domain model (and therefore with TISRIM). This bigger investigation should follow on the more narrow study we did now, but within the current research project there was not enough time and resources to undertake this bigger investigation as well. Conversely, if we had validated directly with ISSRM practitioners not familiar with the ISSRM domain model nor with TISRIM, then we could not have been sure that the outcomes would not have been influenced by the unfamiliarity rather than by our EAM additions. This would have decreased the internal validity of the study, and we would not have been able to verify what we wanted to check: the evolution to the EAM-ISSRM integrated model, the ISSRM domain model as such having already been validated in our previous work [7].

Another threat to descriptive validity [12] is that the subjects, knowing that we designed the EAM-ISSRM integrated model, would be inclined to give a positive evaluation of the model. To mitigate this threat, we made clear that they would not help us more by giving constructive criticisms that indicate weak spots and improvement opportunities in the model. Also, to ask people about their satisfaction of using an ISSRM tool that would be based on our model is a threat to descriptive validity [12], as the answers may not all describe what would actually happen if subjects were to use such a tool. For some questions, they may have answered a median value because of the difficulties the subjects had to imagine using such a tool. Another threat to validity concerning the SUS questionnaire is it generally requires at least 12 subjects to produce “correct” conclusions (100% accurate), but already provides 75% accuracy starting from eight subjects [39]. With nine subjects, we are in the latter case, thus the accuracy can be estimated around 75%.

Lastly, classification of errors in minor and major errors is subject to a threat of descriptive validity, namely the threat of subjective classification. We tried to mitigate this threat by defining the classes as clearly as possible, and by having the classification performed by two members of our group independently. The few cases where the classifiers disagreed, these differences were discussed and resolved by referring back to the definitions of major and minor errors.

8 Related work

The Open Group, in a white paper published in 2015 [51], analyses different approaches to model enterprise risks, as well as security concepts, based on ArchiMate 2.1. It examines a selection of well-established paradigms for risk and security modelling and analyses, extracts a set of core concepts for them, and maps most of the concepts to ArchiMate language elements. However, the scope of this white paper differs from our scope because they also consider non-security risks (strategic, financial, project) with information security risks (i.e. risks harming confidentiality, integrity and availability of information). Moreover, their proposal is ad hoc and not founded on a conceptual model exhaustively covering the addressed domain. Barateiro et al. [52] 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. The paper proposes a risk management framework, including a XML-based domain-specific language for RM (Risk-DL) and explains clearly the link with the ISO 31000 standard [53]. Innerhofer-Oberperfler and Breu [54] propose an approach for the systematic assessment and analysis of IT-related risks in organisations and projects. The goal of the approach is to bridge the different views of the stakeholders involved in security management. They propose an information security metamodel and consider the security management process to be performed by security micro-processes executed by domain owners. In the same way, Ertaul and Sudarsanam [55] propose to exploit the Zachman framework [9] for defining and designing tools for securing an enterprise. This helps, *in fine*, to support security planning especially for IT. SABSA [56] 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 [9], adapted somewhat to a security view. The Open Enterprise Security Architecture guide [30] is a guide providing a comprehensive overview of the key security issues, principles, components, and concepts under-

lying architectural decisions. It provides a framework that serves as a common reference for describing enterprise security architecture and technology. The five preceding references develop conceptual or methodological advances in linking EAM with ISSRM but none of them propose an integrated and complete model for both domains. Goldstein and Franck have proposed a set of 23 requirements a modelling approach should satisfy to deal with IT security design and management [57]. They also integrate security risk with multiple perspectives of the enterprise [58], extending their proprietary modelling framework (MEMO) and its set of domain-specific modelling languages (DSML) to support the management of IT security. We share with them the common objective to define a DSML enhancing an existing method for enterprise modelling. However, their scope is wider than ours, as they address the multiple perspectives of the enterprise, while we focus on the asset perspective. We also promulgate the adoption of standardised EA language (ArchiMate) and do not rely on any specific modelling technology: our conceptual model can be implemented with any technology supporting the definition of a DSML. CORAS [59] is an approach to risk analysis based on ISO 31000 [53]. The approach is model-driven 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 [60]. However, CORAS introduces its own kinds of diagrams and does not rely on EAM models to perform ISSRM. A parallel work from our institution [61] proposes a conceptual mapping of EAM and ISSRM, with the purpose of leveraging the risk as the common instrument to manage the often conflicting objectives associated with IS supporting the delivery of business services. The approach relies on the capabilities of EA to coherently address the multiple views of the enterprise. Although the conceptual mapping is largely shared, we concentrate here on the development of a security risk DSML and its usability for the end-users.

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.

9 Discussion and future work

In this paper, we described how we developed an integrated EAM-ISSRM conceptual model extending the ISSRM domain model [7,12]. The need of such an extension is moti-

vated by a set of drawbacks we observed in traditional ISSRM methods, namely:

- Complexity of IS coming with an increasing number of threats to manage,
- Continuous evolution of organisations and thus of related risks,
- Increasing regulatory pressure, and
- Lack of documentation for ISSRM activities.

Based on the conclusions drawn during the validation of the EAM-ISSRM integrated model, we consider that this model is useful to address the drawbacks identified in traditional ISSRM methods. The model was also assessed as usable for being the conceptual foundation to design our framework (modelling language, method, and tool) to perform ISSRM.

Regarding future work, the EAM-ISSRM integrated model will be used for the definition of a modelling language and of a catalogue of method fragments/chunks (in which methodological aspects and especially risk calculation and assessment will be developed). They will both be integrated in a tool. Through these methodological improvements, the last drawback observed, namely generic aspect of ISSRM methods and lack of guidelines *wrt* the variety of context of use, will be tackled.

Taking care of the concerns of the validation group participants about the complexity of the approach, a particular attention shall be given to keep simple the method and the tool. To ease and reduce the time to be spent on ISSRM activities is also part of our motivations. Once these artefacts designed, the validation will be extended to the *Efficiency* criterion that will help us to measure more precisely to what extent integration of EAM with ISSRM helps to mitigate the drawbacks identified for traditional ISSRM methods. We will indeed be able to measure resources spent by the user to ensure accurate and complete achievements of ISSRM by using our new framework. To conclude on validation aspects, as claimed by Obrst et al., “the ultimate evaluation of an ontology is in terms of its adoption and successful use, rather than its consistency or coverage” [62].

Finally, further than our framework, the EAM-ISSRM integrated model may also be used to provide a better consideration of risk and security aspects in EAM methods. Our objective is only focused on improving ISSRM methods, and the model validation was designed in this way; however, the EAM-ISSRM integrated model might still be promising to improve EAM methods.

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

Appendix 1: EAM-ISSRM Integrated Model Validation—Pretest survey

What are the strengths and the weaknesses in performing ISSRM based on TISRIM and the ISSRM domain model? Is there specific strengths and weaknesses that are related to the concepts at stake?

Strengths:

-
-
-
-
-

Weaknesses:

-
-
-
-
-

Appendix 2: EAM-ISSRM Integrated Model Validation—Exercises

Exercise 1 (40 min)

Case – LuxAssur

For sake of brevity, the full text of the case is not included in the paper⁴. The case is about “LuxAssur”, an insurance company. The management of the company wants to set up an Information Security Management System (ISMS) to improve the global security level of the organization, and make an informed decision for outsourcing parts of the infrastructure. Thus, to do a risk assessment is necessary.

The description of the case is composed of the following parts:

- a) **Presentation:** a general presentation of the LuxAssur company
- b) **Sites:** the physical location of the company and its subsidiaries
- c) **External parties:** the clients and suppliers of LuxAssur
- d) **Information system:** an overview of the IS
- e) **Activities:** the list of business activities performed
- f) **Architecture model:** an architecture model of LuxAssur

Based on the preceding description of LuxAssur, identify in the text or define by yourself in accordance with the case an instance of each concept of the EAM-ISSRM integrated model:

Environment:

Constraint:

Stakeholder:

Asset:

Business asset:

IS asset:

Security criterion:

Security objective:

Business element:

Application element:

Technology element:

Organization:

Location:

Actor:

Risk:

Event:

Impact:

Threat:

Vulnerability:

Attack method:

Threat agent:

Risk treatment:

Security requirement:

Control:

Exercise 2 (20 min)

In the ISO/IEC 27001 standard, identify the set of requirements that are covered by the ISSRM domain model and if there are additional requirements covered by the EAM extension.

Requirements covered by the ISSRM domain model:

Requirements covered by the EAM extension:

SUS Questionnaire: Please complete this questionnaire. The term “system” means an ISSRM tool based on the EAM-ISSRM Integrated Model.

	Strongly disagree				Strongly agree
1. I think that I would like to use such a system frequently	1	2	3	4	5
2. I think that I would find such a system unnecessarily complex	1	2	3	4	5
3. I think such a system would be easy to use	1	2	3	4	5
4. I think that I would need the support of an expert to be able to use such a system	1	2	3	4	5
5. I think I would find the various concepts in such a system well integrated	1	2	3	4	5
6. I think there would be too much inconsistency in such a system	1	2	3	4	5
7. I would imagine that most people will learn to use such a system very quickly	1	2	3	4	5
8. I think that I would find such a system very awkward to use	1	2	3	4	5
9. I would feel very confident using such a system	1	2	3	4	5
10. I would need to learn a lot of things before I could get going with such a system	1	2	3	4	5

Appendix 3: EAM-ISSRM Integrated Model Validation—Post-test survey

Question 1:

Could you recap what are the different concepts that are part of the EAM extension and their linked concepts in the ISSRM domain model? (15min)

Question 2:

What is your general feedback on the EAM extension of the ISSRM domain model? (15min)

References

1. Symantec: Internet Security Threat Report, Volume 21 (2016)
2. PricewaterhouseCoopers: The Global State of Information Security Survey 2016 (2016)
3. Proper, H.A.: Enterprise Architecture—Informed steering of enterprises in motion. In: Proceedings of the 15th International Conference on Enterprise Information Systems (ICEIS) (2013)
4. Official Journal of the European Union: Directive 2009/140/EC of the European Parliament and of the Council of 25 November 2009 (2009)
5. CSSF: Circulaire CSSF 12/544—Optimisation par une approche par les risques de la surveillance exercée sur les “PSF de support” (2012)
6. ISO/IEC 27001:2013: Information technology—Security techniques—Information security management systems—Requirements. International Organization for Standardization, Geneva (2013)
7. Mayer, N.: Model-based Management of Information System Security Risk, PhD Thesis, University of Namur, Namur, Belgium (2009)
8. ISO/IEC 27005:2011: Information technology—Security techniques—Information security risk management. International Organization for Standardization, Geneva (2011)
9. Zachman, J.A.: A framework for information systems architecture. *IBM Syst. J.* **26**, 276–292 (1987)
10. Saha, P.: A Systemic Perspective to Managing Complexity with Enterprise Architecture. 1st edn. IGI Global (2013)
11. Op’t Land M., Proper E., Waage M., Cloo J., Steghuis C.: Positioning Enterprise Architecture. In: Enterprise Architecture, pp. 25–47. The Enterprise Engineering Series. Springer, Berlin, Heidelberg
12. 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., Ralyté, J. (eds.) *Int. Perspect. Inf. Syst. Eng.*, pp. 289–306. Springer, Berlin Heidelberg, Berlin, Heidelberg (2010)
13. 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, Berlin (2015)
14. Wieringa, R.J.: *Design Science Methodology for Information Systems and Software Engineering*. Springer, GmbH & Co. K, Berlin and Heidelberg, New York (2014)
15. Chowdhury, M., Matulevičius, R., Sindre, G., Karpati, P.: Aligning mal-activity diagrams and security risk management for security requirements definitions. *Requir. Eng. Found. Softw. Qual.* **7195**, 132–139 (2012)
16. Matulevičius, R., Mayer, N., Heymans, P.: Alignment of misuse cases with Security Risk Management. In: Proceedings of the 4th Symposium on Requirements Engineering for Information Security (SREIS’08), in Conjunction with the 3rd International Conference of Availability, Reliability and Security (ARES’08), pp. 1397–1404. IEEE Computer Society (2008)
17. Matulevičius, R., Mayer, N., Mouratidis, H., Dubois, E., Heymans, P., Genon, N.: Adapting secure tropes for Security Risk Management during early phases of the information systems development. In: Proceedings of the 20th International Conference on Advanced Information Systems Engineering (CAISE’08), pp. 541–555. Springer, Berlin (2008)
18. Altuhhova, O., Matulevičius, R., Ahmed, N.: Towards definition of secure business processes. In: Bajec, M., Eder, J. (eds.) *Advanced Information Systems Engineering Workshops*, pp. 1–15. Springer, Berlin, Heidelberg (2012)
19. Lankhorst, M. (ed.): *Enterprise Architecture at Work: Modelling, Communication And Analysis*. Springer, Berlin (2005)
20. The Open Group: *ArchiMate® 2.1 Specification* (2013)
21. The Open Group: *TOGAF Version 9.1*. Van Haren Publishing, The Netherlands (2011)
22. Vernadat, F.: Enterprise modeling in the context of enterprise engineering: state of the art and outlook. *Int. J. Prod. Manag. Eng.* **2**, 57 (2014)
23. Peffers, K., Tuunanen, T., Rothenberger, M., Chatterjee, S.: A design science research methodology for information systems research. *J. Manag. Inf. Syst.* **24**, 45–77 (2007)
24. 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)
25. ISO/IEC/IEEE 42010:2011: Systems and software engineering—Recommended practice for architectural description of software-intensive systems. International Organization for Standardization, Geneva (2011)
26. ISO/IEC/IEEE 15288:2015: Systems and software engineering - System life cycle processes. International Organization for Standardization, Geneva (2015)
27. Buckl, S., Schweda, C.M.: *On the State-of-the-Art in Enterprise Architecture Management Literature*. Technische Universität München, München (2011)
28. U.S. Department of Defense: The DoDAF Architecture Framework Version 2.02. <http://dodcio.defense.gov/Library/DoDArchitectureFramework.aspx>
29. van’t Wout, J., Waage, M., Hartman, H., Stahlecker, M., Hofman, A.: *The Integrated Architecture Framework Explained*. Springer, Berlin, Heidelberg (2010)
30. Wahe, S.: *Open Enterprise Security Architecture (O-ESA): A Framework and Template for Policy-Driven Security*. Van Haren Publishing, Zaltbommel (2011)
31. IFIP-IFAC Task Force on Architectures for Enterprise Integration: GERAM: The Generalised Enterprise Reference Architecture and Methodology. In: Bernus, P., Nemes, L., Schmidt, G. (eds.) *Handbook on Enterprise Architecture*, pp. 21–63. Springer, Berlin, Heidelberg (2003)
32. Raymond, K.: Reference model of open distributed processing (RM-ODP): introduction. In: Raymond, K., Armstrong, L. (eds.) *Open Distributed Processing*, pp. 3–14. Springer, New York (1995)
33. Kruchten, P.B.: The 4+1 view model of architecture. *IEEE Softw.* **12**, 42–50 (1995)
34. 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. <http://arxiv.org/abs/1701.01664> (2016)
35. Mayer, N., Aubert, J., Grandry, E., Feltus, C.: An integrated conceptual model for Information System Security Risk Management and Enterprise Architecture Management based on TOGAF. In: *The Practice of Enterprise Modeling? 9th IFIP WG 8.1. Working*

- Conference, PoEM 2016, Skövde, Sweden, pp. 353–361. Springer, Berlin (2016)
36. Schwartz, L., Grandry, E., Aubert, J., Watrinet, M.-L., Cholez, H.: Participative design of a security risk reference model: an experience in the healthcare sector. In: Proceedings of Short and Doctoral Consortium Papers Presented at the 8th IFIP WG 8.1 Working Conference on the Practice of Enterprise Modelling (PoEM 2015), pp. 1–10. CEUR Workshop Proceedings, Valencia, Spain (2015)
 37. Mayer, N., Dubois, E., Matulevičius, R., Heymans, P.: Towards a measurement framework for Security Risk Management. In: Modeling Security Workshop (MODSEC '08). 11th International Conference on Model Driven Engineering Languages and Systems (MODELS '08), Toulouse, France (2008)
 38. Genon, N.: Modelling Security during Early Requirements: Contributions to and Usage of a Domain Model for Information System Security Risk Management (2007)
 39. Wynekoop, J.L., Russo, N.L.: Studying system development methodologies: an examination of research methods. *Inf. Syst. J.* **7**, 47–65 (1997)
 40. Brank, J., Grobelnik, M., Mladenić, D.: A survey of ontology evaluation techniques. In: Proceedings of the Conference on Data Mining and Data Warehouses (SIKDD) (2005)
 41. Recker, J.C.: Conceptual model evaluation. Towards more paradigmatic rigor. In: Castro, J., Teniente, E. (eds.) CAiSE'05 Workshops, pp. 569–580. Porto, Portugal (2005)
 42. Nielsen, J.: Usability Engineering. Morgan Kaufmann, Burlington (1994)
 43. Cleeff, A.: Physical and Digital Security Mechanisms: Properties, Combinations and Trade-offs. University of Twente, Enschede (2015)
 44. Brooke, J.: SUS—a quick and dirty usability scale. *Usability Eval. Ind.* **189**, 4–7 (1996)
 45. Tullis, T.S., Stetson, J.N.: A comparison of Questionnaires for assessing Website usability. Presented at the Usability Professional Association Conference (2004)
 46. Mayer, N.: A cluster approach to security improvement according to ISO/IEC 27001. In: Software Process Improvement, 17th European Conference, EuroSPI 2010
 47. Mayer, N., Aubert, J.: Sector-specific tool for Information Security Risk Management in the Context of Telecommunications Regulation (Tool Demo). In: Proceedings of the 7th International Conference on Security of Information and Networks, pp 85–85. ACM, New York, NY, USA (2014)
 48. Lewis, J.R., Sauro, J.: The factor structure of the System Usability Scale. In: Kurosu, M. (ed.) Human Centered Design, pp. 94–103. Springer, Berlin, Heidelberg (2009)
 49. Sauro, J.: A practical guide to the system usability scale: background, benchmarks & best practices. Measuring Usability LLC, Denver, CO (2011)
 50. Bangor, A., Kortum, P., Miller, J.: Determining what individual SUS scores mean: adding an adjective rating scale. *J. Usability Stud.* **4**, 114–123 (2009)
 51. Band, I., Engelsman, W., Feltus, C., Paredes, S.G., Hietala, J., Jonkers, H., Massart, S.: Modeling Enterprise Risk Management and Security with the ArchiMate®. Language, The Open Group (2015)
 52. 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)
 53. ISO 31000:2009: Risk management—Principles and guidelines. International Organization for Standardization, Geneva (2009)
 54. Innerhofer-Oberperfler, F., Breu, R.: Using an Enterprise Architecture for IT Risk Management. Presented at the Information Security South Africa 6th Annual Conference (2006)
 55. Ertaul, L., Sudarsanam, R.: Security planning using Zachman framework for enterprises. In: Proceedings of EURO mGOV 2005 (2005)
 56. Sherwood, J., Clark, A., Lynas, D.: SABSA ® Enterprise Security Architecture (2010)
 57. Goldstein, A., Frank, U.: A language for multi-perspective modelling of IT security: objectives and analysis of requirements. In: La Rosa, M., Soffer, P. (eds.) Business Process Management Workshops, pp. 636–648. Springer, Berlin, Heidelberg (2013)
 58. Goldstein, A., Frank, U.: Components of a multi-perspective modeling method for designing and managing IT security systems. *Inf. Syst. E-Bus. Manag.* **14**, 101–140 (2016)
 59. Lund, M.S., Solhaug, B., Stolen, K.: Model-Driven Risk Analysis: The CORAS Approach. Springer, Berlin and Heidelberg; GmbH & Co. K, London, New York (2010)
 60. Solhaug, B., Stølen, K.: 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)
 61. Grandry, E., Feltus, C., Dubois, E.: Conceptual integration of Enterprise Architecture Management and Security Risk Management. In: Enterprise Distributed Object Computing Conference Workshops (EDOCW), 17th IEEE International Enterprise Distributed Object Computing Conference, pp. 114–123 (2013)
 62. Obrst, L., Ceusters, W., Mani, I., Ray, S., Smith, B.: The Evaluation of Ontologies. In: Baker, C.J.O., Cheung, K.-H. (eds.) Semantic Web, pp. 139–158. Springer, US (2007)



Nicolas Mayer (<http://www.nmayer.eu>) is Senior Research & Technology Associate at the IT for Innovative Services (ITIS) department of the Luxembourg Institute of Science and Technology (LIST). He graduated in 2004 a M.Sc. degree in Computer Science from the University Henri Poincaré (UHP) of Nancy (France) and in 2009 a Ph.D. Degree from the University of Namur, Belgium. Today, he is Principal Investigator of research and industrial projects related to Information Security, Risk Management, IT compliance and Enterprise Architecture Modelling.



Jocelyn Aubert is Research & Technology Associate at the IT for Innovative Services (ITIS) department of the Luxembourg Institute of Science and Technology (LIST). He obtained two Master degrees, one in IT Security Management from the University of Luxembourg (Luxembourg) and the second in Human-computer interaction from the University of Lorraine (France). His main interests are research and development in software systems, IT Security, risk management tools and methodologies, critical infrastructures monitoring, access control and trust.



Eric Grandry is product manager at the Luxembourg Institute of Science and Technology (LIST). He has extensive R&D experience in model-driven engineering (MDE), software architecture and enterprise architecture (EA), both in research institutes (Vrije Universiteit Brussels, and LIST) and commercial companies (Banksys, Clearstream Services, OneTree Technologies). His research field is the management of complex socio-technical systems by leveraging MDE approaches, in vari-

ous domains: financial services, telecommunications, healthcare, public administration. He is currently more specifically designing model-based methods and technology to address regulatory compliance in the financial industry (RegTech), including regulatory reporting and risk management. He is leading the design of reference architectures to realize the European Digital Single Market, more specifically in the context of the Large Scale Pilots e-SENS (consolidating generic IT solutions to support cross-border public services), and TOOP (addressing The Once Only Principle in the context of cross-border businesses). He is contributing to the open source JSMF project (<https://js-mf.github.io/>), a web-based flexible modelling framework.



Christophe Feltus is graduated as an Electromechanics Engineer from the Institut Supérieur Industriel des Art et Métiers Pierrard (Belgium) and Doctor of Science (Computer Science) from the University of Namur (Belgium). He worked for several years in private companies as: Production Head at Pfizer SA in Jette, Project Coordinator at Nizet Entreprise in Louvain-la-Neuve, and Assessor for the Civil Belgium Aviation Administration in Brussels, Belgium. In 1999, he joined the Lux-

embourg Institute of Science and Technology (formerly the Public Research Centre Henri Tudor) in the Grand-Duchy of Luxembourg to work in the field of Service Science and Innovation. There he has taken part in projects related to IT security, IT governance, business IT/alignment, and Enterprise Architecture modelling.



Dr. Elio Goettelmann received his M.Sc. from the University of Lorraine, Nancy, France in 2011. He graduated as a Ph.D. in computer science at the same university in 2015. Currently he is working as a R&D engineer at the Luxembourg Institute of Science and Technology. His main research interests are Business Process Management, Security Risk Management, and Cloud Computing. He published various papers about these topics since the beginning of his thesis in 2012.



Roel Wieringa (<http://www.cs.utwente.nl/~roelw>) is Chair of Information Systems at the University of Twente, The Netherlands. Over the past 30 years he has done research in several aspects of formal specification of database constraints, requirements engineering and conceptual modeling for information systems, design of e-business networks, IT security risk assessment, and the design of situation-aware platforms for decentralized coordination. He has written three text-

books, *Requirements Engineering, Frameworks for Understanding* (Wiley 1996), *Design Methods for Reactive Systems* (Morgan Kaufmann 2003), and *Design Science Methodology for Information Systems and Software Engineering* (Springer, 2014). He has been Associate Editor in Chief of *IEEE Software* for the area of requirements engineering from 2004 to 2007, scientific director of the Dutch national School for Information and Knowledge Systems from 2006 to 2011 and chair of the Computer Science Department of the UT from 2009 to 2012. In 2017 he co-founded *TheValueEngineers.nl*, which provides software and gives advice about designing sustainable and robust e-business models.