2019 IEEE International Conference on Cloud Computing Technology and Science (CloudCom)

Towards an Integration of Information Security Management, Risk Management and Enterprise Architecture Management – a Literature Review

Thomas Diefenbach
Department of Computer Science
Bundeswehr University Munich
Munich, Germany
thomas.diefenbach@unibw.de

Carsten Lucke
Center of Competence for
Information Technology
Technische Hochschule Mittelhessen
University of Applied Sciences
Friedberg, Germany
carsten.lucke@mnd.thm.de

Ulrike Lechner
Department of Computer Science
Bundeswehr University Munich
Munich, Germany
ulrike.lechner@unibw.de

***Abstract*— Organizations are faced with an increased number of security-related challenges. Our research interest is on information security matters with our proposition being that enterprise architecture management (EAM) can support risk management (RM) and information security management (ISM) for instance by providing a plethora of information about an organization's information assets. We conducted a literature review, which underlines our proposition. The pivotal question we aim to answer is how EAM, RM and ISM efforts can be integrated for "the greater good", i.e., to achieve a facilitation of RM and ISM through the adoption of EAM. As a result, we present an integrated conceptual model which places our findings in the context of the well-established concepts defined in ISO-27001, ISO-31000 and ISO-42010.**

Keywords*— *information security, it security, risk management, enterprise architecture, literature review

I. Introduction

Information security is gaining importance, especially in business environments. In 2017, the largest stand-alone writer in U.S. cyber insurances market – American Int'l Group (AIG) – dealt with as many claims notifications as in 2013 to 2016 combined, the top cause of reported incidents being cyber-attacks [1,2]. Also, organizations have to be compliant to an increasing number of regulations – like, e.g., the General Data Protection Regulation (GDPR) [3] introduced in the European Union (EU) in May 2018.

In general, digitalization and intertwined compliance areas drive the significance of information security in organizations. One might say, not too long-ago risks related to information security had a maintainable risk-damage for the underlying organization. Nowadays organizations are facing the fact, that information security-related risks can no longer be seen as isolated from their core business, but that they can form an existential threat.

We see a clear need for information security management (ISM) to take a variety of perspectives on an organization and to consider different aspects reaching from organizational structure over processes to information systems and their underlying implementation and technologies. However, such an overarching approach would need to have access to a plethora of information about an organization. The associated costs for such an all-embracing ISM approach would be considerable, which, in ISM practice, leads to an on-demand collection of information when needed.

We propose, that this lack of a holistic view on the security-related information and information provision can be addressed through the adoption of enterprise architecture management (EAM). In EAM, approaches for gathering and describing enterprise assets are already well-researched and in place, whilst in risk management (RM) this is still challenging due to different efforts operating in narrowly focused silos, lacking an organization-wide view of risks [4]. The idea of empowering enterprise risk and information security management through the adoption of EAM raises hopes for synergetic effects.

To understand the current state of research in the field of these adjacent domains, we conducted a structured literature review and searched for existing contributions describing facilitation of RM and ISM through adoption of EAM. We identified and analyzed 46 research papers. We describe and place our findings in the context of concepts from established standards, i.e., ISO-27001 [5], ISO-31000 [6] and ISO-42010 [7], as well as present an integrated conceptual model.

This paper is structured as follows. In the next section, the theoretical foundations of our research will be presented. We describe our method in section III and discuss our results in section IV. A conclusion in section V ends this paper.

II. Foundations: Risk Management, Information Security Management and Enterprise Architecture Management

Subsequently we give a brief introduction to the domains of risk management, information security management and enterprise architecture management, these being the relevant fields of research in regard to our research question posed in section II.C

A. Risk Management and Information Security Management

Risk management (RM) is well discussed, both, in academia and corporate practice. According to ISO-31000 [6] RM is defined as "coordinated activities to direct and control an organization with regard to risk" with a risk being an "effect of uncertainty on objectives". There are several RM frameworks and best practice approaches, of which three will be mentioned here, because of their relevance in practice: First, the *ISO-31000* [6], which provides principles, a framework and a process for managing risk in various kinds of organizations [6]. Second, *M_o_R | Management of Risk* [8] issued by AXELOS, an organization also managing best

2330-2186/19/$31.00 ©2019 IEEE
DOI 10.1109/CloudCom.2019.00057

practices like ITIL and PRINCE2. Third, COSO-ERM [9], a risk management approach quite popular in the U.S. being issued from *The Committee of Sponsoring Organizations of the Treadway Commission* (COSO). Typically, these frameworks define a set of principles/guidelines and a process for managing risk in various kinds of organizations. Although certain steps might differ, an RM process typically consists of *risk assessment*, comprising e.g., a set of techniques to identify, analyze and evaluate risks, followed by *risk treatment*.

Closely related to RM is information security management, which shall preserve the confidentiality, integrity and availability of information – objectives commonly known as the CIA triad of information security – by applying a risk management process [5]. Thus, for ISM typically some kind of RM approach is adopted. This might be a general RM framework (like the aforementioned ISO-31000) or an ISM-specific RM framework might be used. ISO-27001 for instance refers to ISO-27005 [10] for RM. ISO-27005 presents procedures specifically adapted to the ISM domain but also adheres to practices and recommendations made in the more general ISO-31000. ISM specifics like the control objectives and controls catalog in ISO-27001 (cf. [5], Annex A) are then tied in, to allow for information security-specific considerations.

B. Enterprise Architecture Management

Following Schelp and Winter [11] EAM establishes centralized, top-down driven, enterprise-wide governance mechanisms that aim at maintaining transparency, coherency, and ultimately flexibility of enterprise architecture (EA). EA is understood as "the fundamental organization of [an enterprise] embodied in its components, their relationships to each other, and to the environment" [7]. Enterprise architecture descriptions (EAD) in conformance to stakeholder-dependent viewpoints, help to illustrate an organization's architectural information [7].

One may assume, that EAM can support RM and ISM by acting as information basis on an organization's "fundamental organization". Whether for general RM or for ISM, one will need a plethora of information about his or her organization to accomplish both, proper risk assessment as well as successful risk treatment (i.e., two of the main RM processes [6]). ISO-27005 [10] Annex B serves as a good example in regard to this assumption. It gives advice for identification and valuation of assets (see ISO-27005 for a comprehensive list) and impact assessment. EAM may at the least aid with the identification of assets. If an organization maintains a baseline description of its enterprise architecture, the information security manager will be happy to use it to identify primary assets (i.e., business processes and information) or supporting assets (e.g., hardware, software, network) according to ISO-27005. We consider this example as an initial corroboration to our proposition that EAM can be a facilitator for risk and information security management efforts.

Another important aspect are architectural viewpoints. A viewpoint is a "work product establishing the conventions for the construction, interpretation and use of architecture views" [7]. In other words: a viewpoint defines which architecture information becomes part of an architecture description (consisting of architecture views and models), and how it is to be prepared and presented. In the early days of EAM, the discussion about relevant viewpoints towards an organization's structural elements was very prominent (cf. [12]). Following ISO-42010 [7], a viewpoint is chosen based on stakeholders' concerns. Nowadays, security matters are definitely an important concern and some EA frameworks (e.g., SABSA [13]) already pay attention to this development.

C. Research question

For all we know, there is no consolidated overview in existing literature on how enterprise risk and information security management can be empowered through the adoption of EAM. However, as illustrated in sections II.A and II.B., different ways of how EAM can aid RM and ISM can not only be thought of. In fact, EAM frameworks already exist (e.g., SABSA [13]), which are dedicated to RM and ISM.

Our goal with this research is twofold. Firstly, we aim to gather additional qualitative evidence on how EAM is used to empower RM or ISM efforts (effects concerning the other direction of the relationships between EAM and ISM/RM, meaning how ISM and RM activities might have an impact on EAM, are not our focus).

Secondly, based on insights in existing literature, we aim to answer how EAM, RM and ISM efforts can be integrated to facilitate RM and ISM efforts. Figure 1 illustrates the interrelations between the RM and ISM domains as described before and brings EAM into the picture.

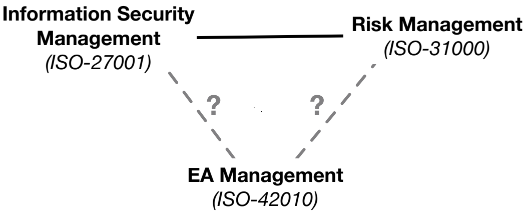

Fig. 1. Research question: interrelations between ISM, RM and EAM

Our goal is to come up with a conceptual idea, on how to integrate commonly accepted frameworks for EAM, RM and ISM (i.e., ISO-27001, ISO-31000, ISO-42010). To do so, we conducted a literature review, following the method presented in the next section.

III. Method

We based the general design of our literature review on recommendations made by Webster and Watson [14] as well as vom Brocke et al. [15]. The first step is deciding which literature to include: As literature databases, we chose *AIS eLibrary*, *IEEE Xplore Digital Library* and *Springer Research & Development*. Furthermore, the proceedings of *Multikonferenz Wirtschaftsinformatik*, *Wirtschaftsinformatik* (both German) and *The Practice of Enterprise Modeling*, as well as the journals *Wirtschaftsinformatik & Management*, *Wirtschaftsinformatik*, *HMD Praxis der Wirtschaftsinformatik* (all three German) and *Business & Information Systems Engineering* were included in our search. We chose these different literature resources to cover a wide spectrum of different research orientations. Our aim was to include practitioner-oriented research as well as scientific communities, both with a topical orientation towards computer engineering as well as literature rather oriented towards the field of information systems.

In the next step, we agreed on keywords for our database-driven literature search. Our keywords are motivated by the three fields of study relevant to our research questions: *Risk Management*, *Enterprise Architecture* and *IT/Information Security*[1]. We conducted separate runs for each database, searching for [*"Enterprise Architecture" AND "IT Security"*] and for [*"Enterprise Architecture" AND "Risk Management"*].

We decided to search literature ranging from Jan. 2007 to Dec. 2018. The results of the database literature search runs are summarized in Table 1.

TABLE I. OVERVIEW OF LIT. DATABASES SEARCH RESULTS

	AISel	IEEE Xplore	Springer
Enterprise Architecture AND IT Security	598	442	136
Enterprise Architecture AND Risk Management	665	201	434

Across these searches, we encountered occurrences of duplicate articles (i.e., 453) as well as entries of a different kind than research papers (e.g., books' front or back covers, in total 107), which were also removed.

Both, the proceedings of the three conferences as well as the four journals were not searched using a search engine. Instead, for the conference proceedings the first author looked manually for possibly relevant conference tracks and then checked if the tracks' contributions' titles seemed to be relevant in consideration of the research questions. Likewise, for the journals, indexes were screened for potentially relevant contributions based on their titles. In total 270 candidates were added to the list. Adding the results of the search runs (2,476 – 453 – 107 = 1,916) to the 270 manually identified papers, a total of 2,186 research contributions were the result of this step.

Each contribution's title and abstract were read to determine its relevance and remove all non-relevant articles. Relevance was given, when the abstract gave hint to a research contribution covering EAM interrelated with RM or ISM respectively. When in doubt about a paper's relevance after reading the abstract, the paper was kept on the list. After completing this step, 64 papers remained for analysis.

For content analysis, we developed a template to record the essential meta information and contents of each paper in a unified schema. Raw material was summarized but remained at least as detailed, to understand the main arguments. Following Mayring such kind of summarization is a valid approach in content analysis when working with rather extensive source material [16].

The first author read all articles and prepared a template for each article, as described. All templates were read by the second author and discussed between first and second author. The goal was to identify and agree on statements being made, hinting on a facilitation of RM or ISM through the adoption of EAM. We differentiated between directly articulated benefits of EAM adoption (i.e., which were pointed out by the respective authors themselves) and indirect benefits, where a benefit was not explicitly articulated by the authors but seems given and reasonable due to the contextual description. We assigned keywords which – by abstraction and aggregation – were iteratively refined to approaches, concepts or interrelations between concepts. In case of non-congruent appraisal, consent was reached by continued discussion based on the original contribution. During content analysis 18 papers were removed from the list of articles for not fitting the scope of research, leaving a total of 46 remaining articles, being research contributions on how EAM can support risk or information security management.

IV. RESULTS

By conducting the literature review, we aimed to gain qualitative evidence on how a facilitation of ISM and RM may be achieved through the adoption of EAM. By abstraction and aggregation during literature analysis, we deduced three central findings. We describe each finding in a separate section from IV.A to IV.C. In section IV.D we will be putting our findings in the context of well-established concepts defined in ISO-27001, ISO-31000, ISO-42010. The resulting model suggests a way of integrating these respective domains.

A. Provision of Architecture-related Information

According to our literature analysis, EAM supports ISM/RM in two ways: (1) by providing input information for risk assessment, since risk assessment heavily relies on information about ISM-relevant assets, and (2) by allowing for a traceback of identified risks to organizational assets in an EA. The majority of identified research focuses on supporting risk assessment [17-30], while a slightly smaller number of contributions discuss the potentials of supporting risk treatment-related activities [4, 18, 23, 29, 31-36].

The following contributions describe the adoption of EAM for risk assessment: First, utilization of EADs to improve calculation results of attack trees and attack defense trees [19, 20, 30] is a topic. Second, business requirements (business goals, to be precise) are included in attack defense trees calculations through the use of EAM [21, 26, 27]. Third, some approaches adopt EA information to live up to the Security by Design (SbD) paradigm in systems development, so that developers can gather information on security-related aspects and take these into account at the beginning of an EA asset's lifecycle [33-37] (e.g., an information system or parts thereof). A central aspect is, that synergetic effects may be achieved by avoiding redundant information retrieval work in ISM/RM when building on information provided by EAM. In this regard, some contributions discuss negative effects that silo-based ISM and RM activities can have and highlight, how integration in this field can enhance quality of RM and ISM efforts [4, 18, 42, 43].

Risk treatment can not only benefit from an "EA-informed" risk assessment but may itself add information to an EA repository. For example, instead of managing risks only with risk registers or similar means, through the integration with EAM a risk traceback can be established by linking treatment information to assets in an EA. We identify contributions where a risk traceback to assets in an EA is done, to support transparency and monitoring of known risks in the

[1] Since terminological heterogeneity of information security vs. IT security vs. * security is a challenge (cf., [67]), for our literature search we decided to use "IT Security" as search term instead of "information security", since in interrelation with enterprise architecture more often – especially with earlier publications – there is a bearing towards "IT", being perceivable (e.g., to be noticed in the adoption of acronyms like EITA for Enterprise IT Architecture even when referring to the whole of viewpoints on an EA, not just matters of "IT").

treatment phase [4, 18] and thereby to improve the data basis for preparation and making of decisions [32].

Another direction of research we identify is the mapping of concepts from EAM to ISM/RM and vice versa. Thus, an asset in the ISM/RM domain can correspond to an architectural element captured in an EAD [18, 38-40]. Such mappings are important to establish how information provision for ISM/RM can be ensured through an EAD. Also, researchers deal with the question of how methods and modeling languages can be integrated or mapped to each other to simplify information exchange between domains (i.e., ISM, RM and EAM) [17]. Some articles focus on "developing and adapting security analysis frameworks to architectural languages" [21, 25]. To conduct a system quality analysis, two contributions extend the ArchiMate modeling language's underlying meta-model. This way, the ability to perform analyses regarding information security objectives like CIA is achieved [24, 25]. One contribution, in a similar regard, introduces an ontological mapping between the COBIT 5 framework and ISO 27001 [41].

B. Integration of Information Security Matters with EA Viewpoints and Frameworks

Apart from the aspect of improved information exchange across domains, we identify several contributions focusing on the inherent integration of information security matters and EAM, which is done on a meta-model level and does especially concern EA viewpoints and EA frameworks (EAF). Current EAF and modeling languages do not meet these needs in full, which is why existing research is exploring how to close this gap. We separate between "long-established" viewpoints and security viewpoints as well as "long-established" EAF and security-focused EAF (i.e., ESAF, see next paragraph). Long-established EAF frequently discussed were the Zachman framework [25, 32, 44, 45], TOGAF [40], DoDAF [25] and the QASAR framework [34]. These publications explore if and how these frameworks can provide a benefit for information security, respectively, which framework alterations or extensions would be necessary to do so.

A more recent stream of literature is on enterprise security architecture frameworks (ESAF) which have an inherent focus on an enterprise's security matters and provide necessary concepts to model and describe security-relevant information. Besides the most quoted ESAF by far – which is SABSA [43, 45-49] – we came upon E2AF [50], RISE [29, 47], AGM [31, 47], ENTRI [51], Gartner EISA Framework [45, 47], ISRUP [36] and SEAST [52].

Along with these two classes of frameworks viewpoints and meta-models are discussed often as well (cf. [31, 46, 53]). One aspect is the extension of long-established EAF with viewpoints focused on enterprise security. Another aspect is the question which viewpoints a "security-native" EAF should define and how an integration with other (more traditional) viewpoints is achieved.

Closely related to the EAF and viewpoint discussion are modeling languages and we found a number of publications on modeling security aspects. Numerous articles discuss security modeling with ArchiMate [17, 25, 54, 55] as well as the ArchiMate's Risk and Security Overlay [56, 57], but also specifically designed languages like P2CySeMoL [19, 30], BMM RAMN [23], pwnPr3d [58] or security-related ontologies [59]. Also the usage of commonly known languages like UML [35-37, 44, 60] and XML [4, 18, 61] to model a variety of security aspects such as security goals and requirements, security activities and processes as well as dependencies among them is part of current research.

C. Widening the Scope of Requirements Engineering in EA Management

Our third central finding is about requirements engineering (RE) in EAM. The importance of RE is already commonly accepted in the EAM community and EAM process models take this fact into account (cf. TOGAF ADM [62] or other widely accepted process models). However, we identified a number of contributions, widening the scope of RE in EAM to consider security-related requirements. Security requirements can be connected to assets in the ISM or RM domain as well as to elements managed in EAM (e.g., processes or information systems) [39].

According to our literature analysis, information security-related requirements may stem from one of three categories: (a) business goals respectively business requirements, (b) legislation necessitating legal requirements or (c) security requirements, which evolve either from conducting own assessments or spring from external sources providing security expertise.

Business requirements already play an important role in EAM and have been discussed by different authors (e.g., [62-64]). However, in our literature analysis we found a number of different articles drawing a connection between business requirements and security requirements, which is a "new flavor" in EA-related requirements engineering. Business requirements can be and are in fact used to identify associated security requirements. This helps "the detection of constraints and security requirements at the information system level, and analyze the risks at the system architecture level in the context of alignment between business and IS" [65]. In section IV.A we have already given an example for the adoption of business requirements for risk assessment.

Legal requirements are dealt with in Samaras et al. [49] in the adoption of SABSA to architect an enterprise IS landscape in accordance to legal requirements and ensure fulfilment of these requirements with the support of models.

Both, business and legal requirements may be used to derive security requirements (cf. [49, 66]) or they can originate from outside organizational borders (e.g., vulnerability databases). Security requirements may for instance be used to support risk assessment methods based on threats' success probability calculations [20].

Awareness about these three kinds of requirements is important for architecture design and, as literature suggests, eventually has positive effects for engineering projects from the very beginning of a software development lifecycle [33, 60].

D. Integrating ISM (ISO-27001), RM (ISO-31000) and EAM (ISO-42010)

In this section we present our integrated conceptual model based on ISO-27001 (plus ISO-27005), ISO-31000 and ISO-42010 (cf. Figure 2). We choose these widely accepted standards since we deem them to be good representatives covering the conceptual foundations in ISM, RM and EAM. We discuss the findings we presented in the previous three sections, in the context of this model and reason about the

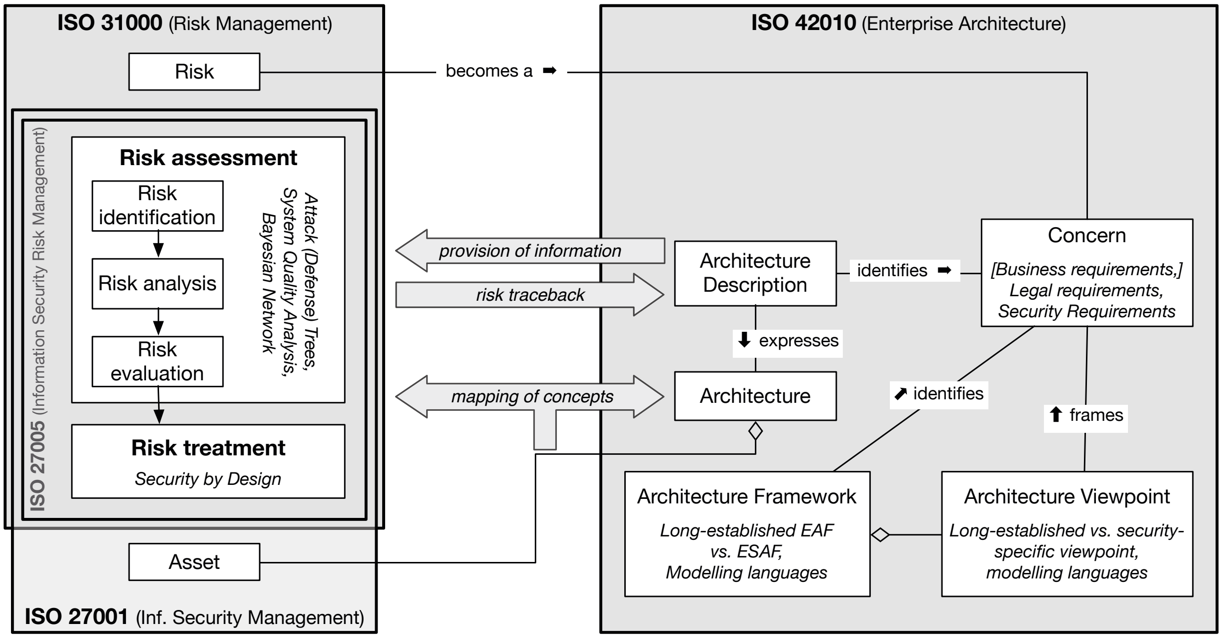
ISO 31000 (Risk Management)
Risk
becomes a ➡
ISO 42010 (Enterprise Architecture)
ISO 27005 (Information Security Risk Management)
Risk assessment
Risk identification
Risk analysis
Risk evaluation
Attack (Defense) Trees, System Quality Analysis, Bayesian Network
Risk treatment
Security by Design
provision of information
risk traceback
mapping of concepts
Architecture Description
identifies ➡
Concern
[Business requirements,] Legal requirements, Security Requirements
⬇ expresses
Architecture
⬈ identifies
⬆ frames
Architecture Framework
Long-established EAF vs. ESAF, Modelling languages
Architecture Viewpoint
Long-established vs. security-specific viewpoint, modelling languages
Asset
ISO 27001 (Inf. Security Management)

Fig. 2. Integration of ISO-27001, ISO-31000, ISO-42010

integration of the given standards respectively the concepts defined by these standards. In the model we use italic script to highlight the findings presented in section IV.A to IV.C. A finding may be directly related to a concept in which case the describing text is placed in the concept rectangle itself. For three findings, however, we preferred to use annotating arrow symbols (i.e., provision of information, risk traceback and mapping of concepts). These are not to be understood as actual elements of the conceptual model. Note, that in this section, we will be focusing on the aspect of integration, which means that we will not be repeating details regarding the findings presented in section IV.A to IV.C.

Be aware that the model in Figure 2 may resemble conceptual models from the standards' documents but does, however, not include all of the concepts present in the original conceptual models. We included only those concepts in connection to our findings, which are thus required to illustrate the big picture and reason about integration aspects. We will also refrain from giving elaborate explanations for established concepts described in these standards, since details may be gleaned from the standards' documents itself.

The first thing to be mentioned is the overlap of ISO-27001, ISO-27005 and ISO-31000. This reproduces that ISO-27001 refers to ISO-27005 for risk management, which presents an approach specifically adapted to ISM but also adheres to the more general ISO-31000. The respective box in the model depicts part of the risk management process presented in ISO-31000 (which is refined in ISO-27005). We added two important concepts to our model: i.e., *Risk* and *Asset*. We decided to put the risk concept in the ISO-31000 box (although also being a core concept in regard to ISO-27005), whereas the asset concept belongs to the ISO-27001 box. We did not add any further concepts like *threat* or *vulnerability*, since neither the discussion of our findings nor our ideas of integration require it, so far.

The concept of asset is very important in regard to the *provision of architecture-related information* (see section IV.A). According to ISO-27005 (see [10], Annex B) there are primary assets (i.e., business processes, information) and supporting assets (i.e., hardware, software, network, personnel, site and organization's structure). These things can be considered part of the organization's architecture. Thus, they can also be expressed through elements in an (enterprise) architecture description. An EAD may then be utilized as a basis for information provision during RM processes. As described in section IV.A this is mainly done for risk assessment but can benefit other RM processes as well. EADs can also be used for risk traceback, which allows for a traceback of identified risks (and other risk-related information) to organizational assets in an EAD as a matter of risk treatment (cf. section IV.A). Thereby, decision-making on the basis of EADs may be facilitated.

For both, the provision of information as well as risk traceback to work, assets must be manageable as part of the (enterprise) architecture. For this to be done, a mapping of concepts is an important premise. EAM frameworks typically define an underlying meta-model (sometimes called information model), that describes its meta-types and associations. Any type of asset must be relatable to a certain type in the EA meta-model. In our conceptual model this only concerns the asset concept. However, if any other concept from the standards on the left side should be managed as part of the architecture or be described in an EAD, it would require such a mapping as well.

Another essential insight of our literature analysis is the necessity and the given willingness, to *widen the scope of requirements engineering in EAM and consider security-related requirements* (cf. section IV.C). According to our findings, important types of requirements to be considered by EAM are legal requirements and security requirements. In this regard, the central concept in ISO-42010 is the architecture-related *concern*, which is defined as "interest in a system relevant to one or more of its stakeholders" [7]. Concerns are motivated by requirements and should be framed by viewpoints / identified by EAF. In our model, the fact that the standards on the left side act as source of security-related requirements which in turn motivate concerns in EAM is modelled through the risk concept in ISO-31000 which exhibits a relation to the concern concept in ISO-42010 (risks become architecture-related concerns).

In our integrated model, architecture viewpoints and frameworks are connected to the risk concept via a transitive relationship. This means that the *integration of information security matters and EAM* (cf. section IV.B) to a high degree concerns architecture frameworks and viewpoints. As discussed in section IV.B, according to our findings, EA frameworks may be divided in long-established EAF and ESAF. A similar aspect applies to architecture viewpoints (long-established vs. security-specific viewpoints). When referring to long-established frameworks and viewpoints we mean frameworks and viewpoints which are per se security-agnostic. The message is: EAM with the claim to facilitate RM and ISM will have to consider security-related requirements and concerns emerging from these requirements, by providing frameworks which identify these concerns and offer suitable viewpoints framing them. Framework designers should take this into account if their frameworks are supposed to be useful for ISM and RM matters.

The discussion about modeling languages is closely related to both topics, frameworks as well as viewpoints. Viewpoints establish conventions for the construction, interpretation and use of architecture views and models (cf. [7]). For a modeling language to be useful for security matters, RM and ISM-related concerns are of high importance, as well, since it must support the modeling of aspects related to these concerns.

V. Summary and conclusion

For the paper at hand, we conducted a structured literature review to reach two research goals: (1) gathering qualitative evidence on how EAM is used to facilitate RM or ISM efforts; (2) answering the question on how EAM, RM and ISM can be integrated to facilitate RM and ISM efforts.

We found a number of 46 contributions which either directly state a positive support of RM and ISM through adoption of EAM or allow for an interpretation that such a support is existent. The approaches described in these publications are summed up by three main themes that we identified in literature (cf. section IV.A to IV.C). Firstly, EAM supports information security by provisioning architecture-related information; it also allows for a traceback of identified risks to organizational assets in an EA as a matter of risk treatment. Secondly, we identified contributions working on extensions and adaptations of EA frameworks, meta-models as well as modeling languages, all aiming to integrate information security matters with EA viewpoints and frameworks. Thirdly, the importance to widen the scope of requirements engineering in EAM to consider legal and security requirements is highlighted. Such requirements should be represented by architecture-related concerns and motivate viewpoint definition in EAM. In view of our findings, we consider it safe to claim, existing literature clearly shows, that EAM indeed facilitates ISM and RM.

In section IV.D we suggest a conceptual model which aims to answer our pivotal question, how ISM, RM and EAM may be integrated (ISO-27001, ISO-31000 and ISO-42010 with their well-established concepts are chosen as representatives for ISM, RM and EAM). We use the model to illustrate how our findings from section IV.A to IV.C are related to each other. Our model shows, that the three commonly used international standards – ISO-27001, 31000 and 42010 – show overlap in their concepts. So far, the purpose of our model is mainly descriptive. However, it can be considered as a good starting point for the development of the conceptual foundation for an integrated management framework which might combine an even larger number of standards with the goal to achieve synergetic effects especially in information collection and information provision. We believe, with organizations striving to be efficient and effective, it is counterintuitive to waste valuable resources by handling these three approaches independently. We also believe, with further refinement, our model could provide a valuable conceptual foundation for GRC (governance, risk management and compliance) software, that supports an integrated approach.

In our opinion, further research could focus on the following aspects: Considering provision of information, it should be established, what information is typically needed for ISM and RM to allow for efficiency in practice and to avoid collection of duplicate data in the name of security. In terms of integration of information security matters with EA viewpoints and frameworks, we believe, the focus should be on integrated frameworks. Having security-specific and security-agnostic frameworks side by side would probably further the proliferation of EA framework and cause unnecessary tailoring and integration efforts on the user-side, which should be avoided. In regard to widening the scope of RE in EAM, we believe the discussion should be about architecture-related concerns emerging from typical security requirements. Here, we see a connection to the question of "what are typical security-viewpoints", that certainly also is a key to the task of integrating security matters into EA frameworks.

As for all qualitative research, further empirical prove would of course be beneficial. However, we believe to have chosen a good variety of literature databases, journals and conference proceedings, which provide a reasonable mixture between practice and research.

References

[1] Insurance Journal, "U.S. Cyber Market Is $2 Billion, Growing Fast, Profitable: Fitch," 2018. [Online]. Available: https://www.insurancejournal.com/news/national/2018/05/10/488833.htm. [Accessed: 01-May-2019].

[2] American International Group, "Cyber insurance claims: Ransomware disrupts business," 2018. [Online]. Available: https://www.aig.co.uk/insights/cyber-ransomeware-disrupts-business. [Accessed: 01-May-2019].

[3] The European Parliment and The Council of the EU, REGULATION (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (GDPR), vol. 59. 2016, pp. 1–88.

[4] J. Barateiro, G. Antunes, and J. Borbinha, "Manage risks through the Enterprise Architecture," in Hawaii International Conference on System Sciences, 2012, pp. 3297–3306.

[5] International Organization For Standardization, "ISO/IEC 27001 - Information technology - Security techniques - Information security management systems - Requirements." 2013.

[6] International Organization For Standardization, "ISO 31000 - Risk management." 2018.

[7] International Organization For Standardization, "ISO/IEC/IEEE 42010 - Systems and software engineering - Architecture description." 2011.

[8] AXELOS, "What is Management of Risk?," 2018. [Online]. Available: https://www.axelos.com/best-practice-solutions/mor/what-is-mor. [Accessed: 01-May-2019].

[9] Committee of Sponsoring Organizations of the Treadway Commission, “Enterprise Risk Management Integrating with Strategy and Performance.” 2017.

[10] International Organization For Standardization, ISO 27005 - Information technology - Security techniques - Information security risk management. 2018.

[11] R. Winter, “Establishing ‘Architectural Thinking’ in Organizations,” in The Practice of Enterprise Modeling, 2016, vol. 197, pp. 3–8.

[12] R. Winter and R. Fischer, “Essential layers, artifacts, and dependencies of enterprise architecture,” in 10th IEEE International Enterprise Distributed Object Computing Conference Workshops, 2006.

[13] The SABSA Institute C.I.C, “SABSA Executive Summary,” 2018. [Online]. Available: https://sabsa.org/sabsa-executive-summary. [Accessed: 01-May-2019].

[14] J. Webster and R. T. Watson, “Analyzing the Past to Prepare for the Future: Writing a Literature Review.,” MIS Q., vol. 26, no. 2, pp. xiii–xxiii, 2002.

[15] J. von Brocke et al., “Reconstructing the Giant: On the Importance of Rigour in Documenting the Literature Search Process,” in 17th European Conference on Information Systems, 2009, pp. 2206–2217.

[16] P. Mayring, Qualitative Inhaltsanalyse - Grundlagen und Techniken, 12. Auflag. Weinheim und Basel: Beltz Verlag, 2015.

[17] M. Korman, T. Sommestad, J. Hallberg, J. Bengtsson, and M. Ekstedt, “Overview of Enterprise Information Needs in Information Security Risk Assessment,” in 2014 IEEE 18th International Enterprise Distributed Object Computing Conference, 2014, pp. 42–51.

[18] J. Barateiro and J. Borbinha, “Integrated management of risk information,” in 2011 Federated Conference on Computer Science and Information Systems, 2011, no. 4, pp. 791–798.

[19] D. Marosin, D. van der Linden, and S. Sousa, “A Collaborative Risk Management Framework for Enterprise Architecture,” in IEEE 8th International Conference on Research Challenges in Information Science, 2014, pp. 1–6.

[20] P. Närman, P. Johnson, and L. Nordström, “Enterprise Architecture: A Framework Supporting System Quality Analysis,” in 11th IEEE International Enterprise Distributed Object Computing Conference, 2007, pp. 130–141.

[21] P. Närman, M. Schönherr, P. Johnson, M. Ekstedt, and M. Chenine, “Using Enterprise Architecture Models for System Quality Analysis,” in 12th International IEEE Enterprise Distributed Object Computing Conference, 2008, pp. 14–23.

[22] S. Sousa, D. Marosin, K. Gaaloul, and N. Mayer, “Assessing Risks and Opportunities in Enterprise Architecture Using an Extended ADT Approach,” in 17th IEEE International Enterprise Distributed Object Computing Conference, 2013, pp. 81–90.

[23] T. Sommestad, M. Ekstedt, and P. Johnson, “Combining defense graphs and enterprise architecture models for security analysis,” in 12th IEEE International Enterprise Distributed Object Computing Conference, 2008, pp. 349–355.

[24] K. Gotz, M. Hawley, J. Hird, and C. Machin, “‘CTRL-S’ - A security tool for SESAR’s design-in security approach,” in 2016 11th International Conference on Availability, Reliability and Security, 2016, no. C, pp. 499–502.

[25] J. A. Anderson and V. Rachamadugu, “Managing Security and Privacy Integration across Enterprise Business Process and Infrastructure,” in 2008 IEEE International Conference on Services Computing, 2008, vol. 2, pp. 351–358.

[26] H. Holm, K. Shahzad, M. Buschle, and M. Ekstedt, “P 2 CySeMoL : Predictive , Probabilistic Cyber Security Modeling Language,” IEEE Trans. Dependable Secur. Comput., vol. 12, no. 6, pp. 626–639, 2015.

[27] M. Välja, M. Korman, K. Shahzad, and P. Johnson, “Integrated metamodel for security analysis,” in 48th Hawaii International Conference on System Sciences, 2015, vol. 2015-March, pp. 5192–5200.

[28] M. Ekstedt, P. Johnson, R. Lagerström, D. Gorton, J. Nydrén, and K. Shahzad, “SecuriCAD by foreseeti: A CAD tool for enterprise cyber security management,” in 2015 IEEE 19th International Enterprise Distributed Object Computing Conference Workshops and Demonstrations, 2015, pp. 152–155.

[29] M. Ekstedt and T. Sommestad, “Enterprise Architecture Models for Cyber Security Analysis,” in IEEE/PES Power Systems Conference and Exposition, 2009, pp. 1–6.

[30] Y. Masuda, S. Shirasaka, S. Yamamoto, and T. Hardjono, “Risk Management for Digital Transformation in Architecture Board: A Case Study on Global Enterprise,” in 6th IIAI International Congress on Advanced Applied Informatics, IIAI-AAI 2017, 2017, pp. 255–262.

[31] J. J. Korhonen, M. Yildiz, and J. Mykkänen, “Governance of information security elements in service-oriented enterprise architecture,” in 10th International Symposium on Pervasive Systems, Algorithms, and Networks, 2009, pp. 768–773.

[32] K. Hinkelmann and N. Onufrienko, “Explicitly Modelling Relationships of Risks on Business Architecture,” in eChallenges e-2014, 2014.

[33] W. Houser, “Employing Enterprise Architecture for Applications Assurance,” IT Professional, no. December, pp. 8–11, 2014.

[34] S. Bode, A. Fischer, W. Kühnhauser, and M. Riebisch, “Software architectural design meets security engineering,” in International Symposium and Workshop on Engineering of Computer Based Systems, 2009, pp. 109–118.

[35] L. Dai and Y. Bai, “An Organization-Driven Approach for Enterprise Security Development and Management,” in 2011 Fifth International Conference on Secure Software Integration and Reliability Improvement, 2011, pp. 208–215.

[36] S. Sabouri and A. M. Rahmani, “Novel {Architect@Place} pattern activity in ISRUP framework,” in 7th International Conference on Information Technology, 2010, pp. 598–602.

[37] S. Sabouri and A. M. Rahmani, “Innovative modeling of {Architect@Place} pattern artifacts in ISRUP framework,” 2nd IEEE International Conference on Information Management and Engineering, vol. 3. pp. 230–234, 2010.

[38] J. Barateiro, G. Antunes, and J. Borbinha, “Long-term security of digital information: Assessment through risk management and Enterprise Architecture,” in IEEE EUROCON - International Conference on Computer as a Tool, 2011, pp. 1–4.

[39] K. Supaporn, N. Prompoon, and T. Rojkangsadan, “Enterprise assets security requirements construction from ESRMG grammar based on security patterns,” in Asia-Pacific Software Engineering Conference, 2007, pp. 112–119.

[40] N. Mayer, J. Aubert, E. Grandry, and C. Feltus, “An Integrated Conceptual Model for Information System Security Risk Management and Enterprise Architecture Management Based on TOGAF,” in The Practice of Enterprise Modelling, 2016, vol. 267, pp. 353–361.

[41] R. Almeida, R. Lourinho, M. M. Da Silva, and R. Pereira, “A model for assessing COBIT 5 and ISO 27001 simultaneously,” in 2018 20th IEEE International Conference on Business Informatics, CBI 2018, 2018, vol. 1, pp. 60–69.

[42] E. Grandry, C. Feltus, and E. Dubois, “Conceptual Integration of Enterprise Architecture Management and Security Risk Management,” in 2013 17th IEEE International Enterprise Distributed Object Computing Conference Workshops, 2013, pp. 114–123.

[43] M. Coetzee, “Towards a Holistic Information Security Governance Framework for SOA,” in 2012 Seventh International Conference on Availability, Reliability and Security, 2012, pp. 155–160.

[44] W. Goudalo and D. Seret, “The process of Engineering of Security of Information Systems (ESIS): The formalism of business processes,” in 3rd International Conference on Emerging Security Information, Systems and Technologies, 2009, pp. 105–113.

[45] S. M. Oda, H. Fu, and Y. Zhu, “Enterprise information security architecture a review of frameworks, methodology, and case studies,” Comput. Sci. Inf. Technol., pp. 333–337, 2009.

[46] P. Pleinevaux, “Towards a metamodel for SABSA Conceptual Architecture Descriptions,” in 11th International Conference on Availability, Reliability and Security, 2016, pp. 187–194.

[47] F. Bahmani, M. Shariati, and F. Shams, “A survey of interoperability in Enterprise Information Security Architecture frameworks,” in 2nd International Conference on Information Science and Engineering, 2010, pp. 1794–1797.

[48] C. Magnusson and S.-C. Chou, “Risk and Compliance Management Framework for Outsourced Global Software Development,” in 5th IEEE International Conference on Global Software Engineering, 2010, pp. 228–233.

[49] V. Samaras, S. Daskapan, R. Ahmad, and S. K. Ray, “An Enterprise Security Architecture for Accessing SaaS Cloud Services with BYOD,” in 11th Australasian Telecommunication Networks and Applications Conference, 2015, no. July, pp. 1–6.

[50] S. G. pour Nezami and R. Azmi, “Usage of enterprise architectural framework for information security management in a holistic approach,” in 2011 IEEE International Conference on Computer Science and Automation Engineering, 2011, vol. 3, pp. 6–10.

[51] N. Mayer, E. Grandry, C. Feltus, and E. Goettelmann, “Towards the ENTRI Framework: Security Risk Management Enhanced by the Use of Enterprise Architectures,” in CAiSE 2015 Advanced Information Systems Engineering Workhops, 2015, vol. 215, pp. 459–469.

[52] M. T. U. Ahmed, N. I. Bhuiya, and M. M. Rahman, “A secure enterprise architecture focused on security and technology-transformation (SEAST),” in 12th International Conference for Internet Technology and Secured Transactions, ICITST, 2017, pp. 215–220.

[53] J. Sun and Y. Chen, “Intelligent Enterprise Information Security Architecture Based on Service Oriented Architecture,” in 2008 International Seminar on Future Information Technology and Management Engineering, 2008, pp. 196–200.

[54] E. Dubois and C. Mauger, “Extended architectural models: First steps towards the reconciliation of the ‘soft’ and the ‘hard’ parts of an enterprise,” in 19th IEEE International Enterprise Distributed Object Computing Conference Workshops and Demonstrations, 2015, pp. 125–129.

[55] H. Jonkers and D. A. C. Quartel, “Enterprise Architecture-Based Risk and Security Modelling and Analysis,” in GraMSec 2016 Graphical Models for Security 3rd International Workshop, 2016, vol. 9987, pp. 94–101.

[56] T. Prince Sales, J. P. Andrade Almeida, S. Santini, F. Baiao, and G. Guizzardi, “Ontological analysis and redesign of risk modeling in archimate,” in 2018 IEEE 22nd International Enterprise Distributed Object Computing Conference, EDOC 2018, 2018, pp. 154–163.

[57] N. Mayer and C. Feltus, “Evaluation of the risk and security overlay of archimate to model information system security risks,” in IEEE International Enterprise Distributed Object Computing Workshop, EDOCW, 2017, vol. 2017-Octob, pp. 106–116.

[58] A. Vernotte, P. Johnson, M. Ekstedt, and R. Lagerstrom, “In-depth modeling of the UNIX operating system for architectural cyber security analysis,” in IEEE International Enterprise Distributed Object Computing Workshop, EDOCW, 2017, vol. 2017-Octob, pp. 127–136.

[59] J. Janulevičius, L. Marozas, A. Čenys, N. Goranin, and S. Ramanauskaite, “Enterprise architecture modeling based on cloud computing security ontology as a reference model,” in Open Conference of Electrical, Electronic and Information Sciences, eStream 2017, 2017.

[60] L. Lowis, “Towards automated risk identification in service-oriented architectures,” in Multikonferenz Wirtschaftsinformatik, 2008, pp. 1149–1158.

[61] M. Menzel, I. Thomas, and C. Meinel, “Security Requirements Specification in Service-Oriented Business Process Management,” in 2009 International Conference on Availability, Reliability and Security, 2009, pp. 41–48.

[62] The Open Group, “The TOGAF Standard, Version 9.2 Overview,” 2018. [Online]. Available: http://www.opengroup.org/togaf. [Accessed: 01-May-2019].

[63] C. Lucke and U. Lechner, “Goal-oriented requirements modeling as a means to address stakeholder-related issues in EA,” in 10. Internationale Tagung Wirtschaftsinformatik (WI), 2011.

[64] D. Quartel, W. Engelsman, H. Jonkers, and M. Van Sinderen, “A goal-oriented requirements modelling language for enterprise architecture,” in Proceedings - 13th IEEE International Enterprise Distributed Object Computing Conference, EDOC 2009, 2009.

[65] A. Ullah and R. Lai, “Managing security requirements: Towards better alignment between information systems and business,” in 15th Pacific Asia Conference on Information Systems: Quality Research in Pacific, 2011.

[66] O. González-Rojas, L. Ochoa-Venegas, and G. Molina-León, “Information security governance: valuation of dependencies between IT solution architectures,” in Lecture Notes in Business Information Processing, 2016, vol. 261, pp. 220–223.

[67] S. Richter, T. Straub, and C. Lucke, “Information Security Awareness – eine konzeptionelle Neubetrachtung,” in Multikonferenz Wirtschaftsinformatik, 2018, pp. 1369–1380.