Towards the ENTRI Framework: Security Risk Management Enhanced by the Use of Enterprise Architectures

Nicolas Mayer(✉), Eric Grandry, Christophe Feltus, and Elio Goettelmann

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

Abstract. Secure information systems engineering is currently a critical but complex concern. Risk management has become a standard approach to deal with the necessary trade-offs between expected security level and control cost. However, with the current interconnection between information systems combined with the increasing regulation and compliance requirements, it is more and more difficult to achieve real information security governance. Given that risk management is not able to deal with this complexity alone, we claim that a connection with Enterprise Architecture Management (EAM) contributes in addressing the above challenges, thereby sustaining governance and compliance in organisations. In this paper, we motivate the added value of EAM to improve security risk management and propose a research agenda towards a complete framework integrating both domains.

Keywords: Security risk management · Enterprise Architecture · Governance · Compliance

1 Introduction

Today, a strong emphasis is put on the security of Information Systems (IS) and on the management of security risks. For example, a new national regulation in Luxembourg about records management [1] concentrates on security and authenticity of records, and imposes a risk-based approach to service providers. *CSSF,*[1] as the National Regulation Authority (NRA) for the financial sector, has defined rules that emphasize IS security; the recent regulation "*Circulaire CSSF 12/544*" [2] has introduced a "risk-based approach" for financial service providers. Last but not least, in the telecommunication sector, the service providers have to comply with the EU Directive 2009/140/EC [3], which Article 13a on security and integrity of networks and services constraints Member States to ensure that providers of public communication networks manage the security risks of networks and services.

[1] *Commission de Surveillance du Secteur Financier.*

A. Persson and J. Stirna (Eds.): CAiSE 2015 Workshops, LNBIP 215, pp. 459–469, 2015.
DOI: 10.1007/978-3-319-19243-7_42

Although managing risks is constrained by regulators, modern day enterprises consider their Risk Management (RM) capabilities as an opportunity to drive competitive advantage. In its 2011 study on Global Risk Management [4], Accenture has identified that "*risk management is now more closely integrated with strategic planning and is conducted proactively, with an eye on how [risk management] capabilities might help a company to move into new markets faster or pursue other evolving growth strategies*". From a security perspective, IS Security RM (ISSRM) supports enterprises to adopt cost-effective security measures: security threats are so numerous that it is impossible to act on all and enterprises are looking for a positive Return On Security Investment (ROSI). In this sense, ISSRM plays an important role in the alignment of a company's business with its IT strategy [5].

Beside the increasing regulatory compliance, enterprises have to deal with disruptions that increase the complexity of their environment: the continuous enterprise evolution (planned evolution and/or unplanned and emergent changes), the disruption in the usage of traditional business solutions (*e.g.*, Dropbox), the heterogeneity of the stakeholder's profile and ability to address security risks, etc. In this enterprise "in motion" [6], new security risks constantly appear and new solutions are required to address them.

Enterprise Architecture Management (EAM) have appeared to be a valuable and engaging instrument to face enterprise complexity and the necessary enterprise transformation [7, 8]. EAM offers means to govern complex enterprises, such as, *e.g.*, an explicit representation of the enterprise facets, a sound and informed decisional framework, a continuous alignment between business and IT, and so forth [9].

Given that the ISSRM discipline is not able to deal with this increasing complexity alone (see Sect. 2), we claim in this paper that a connection with EAM (see Sect. 3.1) contributes in addressing the above challenges (see Sect. 3.2), thereby sustaining governance and compliance in enterprises in motion (see Sect. 3.3).

Section 2 describes the background of our work, and focuses on our preceding works and their drawbacks. Section 3 presents the state of the art in the field of EAM, its links with ISSRM and the evolution of RM towards the GRC concept (Governance, RM, and Compliance). Our research objectives are then defined in Sect. 4. Section 5 presents the research method we currently follow. Finally, Sect. 6 is about current state of the research work, conclusion and future work.

2 Background on Information System Security and Risk Management and Problem to be Tackled

In our preceding works, the concepts of ISSRM have been formalised as a domain model, i.e. a conceptual model depicting the studied domain [10]. The ISSRM domain model was designed from related literature [11]: risk management standards, security-related standards, security risk management standards and methods and security requirements engineering frameworks. The ISSRM domain model is composed of 3 groups of concepts: Asset-related concepts, Risk-related concepts, and Risk treatment-related concepts. Each of the concepts of the model has been defined and linked one to the other [11], as represented in Fig. 1.

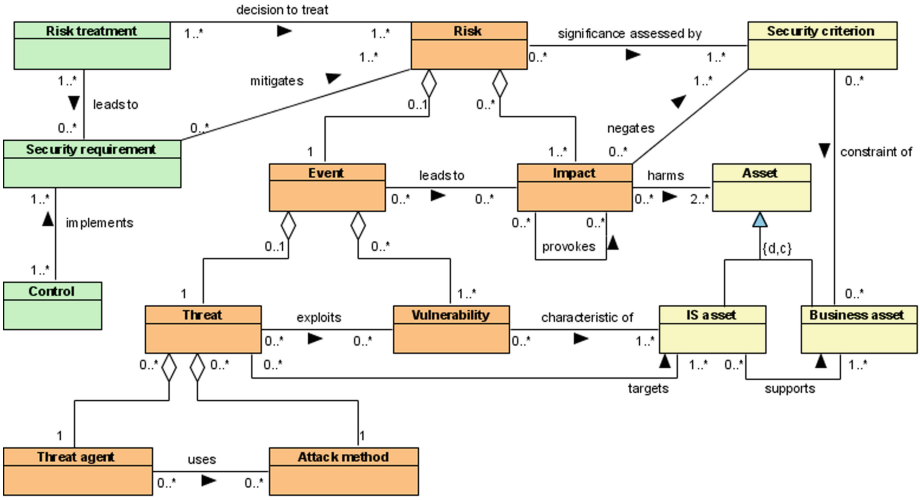

Fig. 1. ISSRM domain model (extracted from [11])

Asset-related concepts 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* describes information, processes, capabilities and skills inherent to the business and core mission of the organisation, having value for it. An *IS asset* is a component of the IS supporting business assets like a database where information is stored. A *security criterion* characterises a property or constraint on business assets describing their security needs, usually for confidentiality, integrity and availability.

Risk-related concepts present how the risk itself is defined. A *risk* is the combination of a threat with one or more vulnerabilities leading to a negative impact harming the assets. An *impact* describes the potential negative consequence of a risk that may harm assets of a system or organisation, when a threat (or the cause of a risk) is accomplished. An *event* is the combination of a threat and one or more vulnerabilities. A *vulnerability* describes a characteristic of an IS asset or group of IS assets that can constitute a weakness or a flaw in terms of IS security. A *threat* characterises a potential attack or incident, which targets one or more IS assets and may lead to the assets being harmed. A *threat 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 describe what decisions, requirements and controls should be defined and implemented in order to mitigate possible risks. A *risk treatment* is an intentional decision to treat identified risks. A *security requirement* is the refinement of a treatment decision to mitigate the risk. *Controls* (countermeasures or safeguards) are designed to improve security, specified by a security requirement, and implemented to comply with it.

After having defined the ISSRM domain model, our contributions has been focused on having a model-based approach for ISSRM. It has been motivated both by an

efficiency improvement of the ISSRM process, and by the enhancement of the product resulting of the performed process [11]. The ISSRM domain model has been successfully applied to analyse different modelling languages: Mal-activity Diagrams [12], Misuse Case [13], Secure Tropos [14], Business Process Modelling Notations [15], and KAOS extended to security [11]. As a general conclusion of these assessments, none of the preceding modelling languages (even when improvements are proposed) is really suited to support the whole ISSRM steps. They are generally focused on a limited number of activities of ISSRM and do not cover its full scope (*i.e.* the business-to-IT stack). Another (related) drawback we observed is that it is generally difficult to model (business and IS) assets in a meaningful manner for ISSRM. In this frame, and as described in the next section, EAM techniques and related benefits are promising to fill these gaps.

3 State of the Art

3.1 Enterprise Architecture Management

Lapalme has extensively reviewed the Enterprise Architecture (EA) literature and has identified three schools of thought, each with its own scope and purpose [16]: Enterprise IT Architecting (EA is the glue between business and IT), Enterprise Integrating (EA is the link between strategy and execution) and Enterprise Ecological Adaptation (EA is the means for organisational innovation and sustainability). Considering the increased competition and disruptions in the markets, Lapalme's taxonomy demonstrates the evolution of EA from an instrument supporting IT and business strategy execution to a management instrument for sustainable innovation and enterprise transformation [17]. As formulated by Op't Land *et al*. [18], the suggested mission of EAM is to add value by providing to the management means for informed governance of enterprise transformation. Next to top-down changes dictated by the strategy, enterprises are subject to a continuous stream of bottom-up changes, which are neither planned nor controlled: from minute adjustments in business processes, simply to make things "work", to the introduction of "shadow IT" (not formally introduced/supported ICT) in the form of cloud services, social media and BYOD.[2] As a consequence, enterprises are in constant motion [19], increasing the governance complexity. EAM, as a management science, provides the optimal platform for managing complexity [8], and making organisations more resilient in the face of disruption, leading to sustainable benefits: Ross *et al*. [20] show how constructing the right EA enhances profitability and time to market, while it improves strategy execution.

EAM is supported by multiple approaches [9, 21–24]. TOGAF [25] is an open EA framework proposed by The Open Group (TOG) and established as a standard. First published in 1995, TOGAF is based on the US Department of Defense Technical Architecture Framework for Information Management (TAFIM). From this sound foundation, TOG's Architecture Forum developed successive versions of TOGAF at regular intervals and published them on TOG's public web site. The framework is

[2] Bring Your Own Device.

mainly composed of a method (the Architecture Development Method, ADM) and a meta-model for architectural artefacts (the Architecture Content Framework, ACF). TOG proposes ArchiMate [26] as a standard EA Modeling Language, providing the capability to represent an enterprise in a uniform way, according to the multiple stakeholders' viewpoints [9]. ArchiMate introduces a layered representation of the EA: business, application and technology. Furthermore, two extensions are introduced since version 2.0 of the language: the Motivation Extension and the Implementation and Migration Extension. The TOGAF framework and the ArchiMate modelling language, as current EA standards, are of particular interest in our context.

3.2 EAM as ISSRM Facilitator

Connecting ISSRM and EAM has been investigated by academic works. Saeki *et al.* [27] underline that EAM is not only for IS/IT planning, but is also an instrument for *corporate planning and business function*, *e.g.*, compliance management or RM. Innerhofer-Oberperfler and Breu [28] propose an approach for a systematic assessment of IT risks using EAM. The goal of the approach is to bridge the different views of the stakeholders involved in security management. They propose an information security meta-model and consider the security management process to be performed by security micro-processes executed by domain owners. In the same way, Ertaul and Sudarsanam [29] propose to exploit the Zachman framework [7] for defining and designing tools for securing an enterprise. This helps, *in fine*, to support security planning especially for IT. Leveraging EAM to defragment the identification of risks and to manage them in an holistic way was also recently proposed in Barateiro *et al.* [30]: EA description is used to model complex business system at the desired level of abstraction, and to cover the views of the enterprise relevant to assess and manage the different kinds of risks. 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 completely integrated approach: modelling language, method and tool.

In terms of industry standards, TOGAF [25] states that the enterprise architects are in good place to identify and mitigate risks. TOG's Architecture Forum is currently investigating the integration of security within EA, making it integrally part of the development of EA, and the ArchiMate Forum investigates extending ArchiMate concepts in order to support risk modelling, notably based on our previous works [31]. We have indeed proposed a conceptual mapping of EAM and ISSRM (first step in conceptual integration) [32] and have demonstrated that ArchiMate can be used to model the subject of the security risk assessment (the assets), but also that security risks and controls can be modelled with the existing ArchiMate constructs. This previous work represents a proof-of-concept in the conceptual integration of ISSRM-EAM: we have indeed identified gaps that require further theoretical and conceptual analysis. These different industrial initiatives confirm the interest of practitioners in the integration of EAM and ISSRM, as well as the need to develop the theoretical foundation for this integration.

3.3 From Risk Management to GRC

Today, RM is part of the integrated GRC concept: Governance, RM, and Compliance. According to the literature [25, 33, 34], "governance" evaluates, directs, and monitors the enterprise strategic objectives. To that end, the corporate governance aims at sustaining the relation between the management, the board of direction, and the shareholders [33, 34]. It also expresses the decision making policies related to corporate issues with the intent to ensure the adequacy of the resources usage according to the strategic objectives of the organisation [35]. The international standard ISO/IEC 38500 [36] is a high level framework that confers guidance on the role of governing body. It provides a set of six high level principles for the managers of the company to help them in evaluating, directing and monitoring the use of the information system of the company. COBIT [37] is a framework that enables the development of clear policies and good practice for IT control throughout enterprises. It is a framework and a supporting toolset that allow managers to bridge the gap with respect to control needs, technical issues and business risks, and communicate this level of control to employees.

GRC is also tackled by academics. Racz *et al*. [38] observe the few existing scientific researches in GRC as an integrated concept, despite the amount of research in the three topics separately. They also identify the main drivers for GRC: the regulatory compliance, followed by RM. The authors define GRC as "*an integrated, holistic approach to organisation-wide governance, risk and compliance ensuring that an organisation acts ethically correct and in accordance with its risk appetite, internal policies and external regulations through the alignment of strategy, processes, technology and people, thereby improving efficiency and effectiveness*". Bonazzi *et al*. [39] propose a process that achieves the regulatory compliance by aligning governance activities and RM. Vicente and da Silva also acknowledge the lack of scientific references related to GRC [40] and define an innovative GRC conceptual model, which strengthens the connections between risk and governance in the sense that governance aims at understanding and foreseeing the vulnerabilities of an organisation. The authors also claim that the alignment between business and risks is enforced by structured governance and compliance management. Another approach [41] proposes to use Situational Method Engineering and method fragments [42] to implement GRC. Once again, in this broader domain of GRC, to the best of our knowledge, there is no extensive and mature research work trying to benefit from research in EAM to improve ISSRM for compliance and governance purpose.

4 Research Objectives

Our proposal aims at connecting RM and EAM, in the area of IS security. We claim that such a connection shall help to reduce GRC complexity and associated cost. Our objective is therefore to answer the following research question (Fig. 2): **How to improve ISSRM using results from EAM for Compliance and Governance purpose?**

To answer this research question, the following objectives with the associated contributions have been specifically defined:

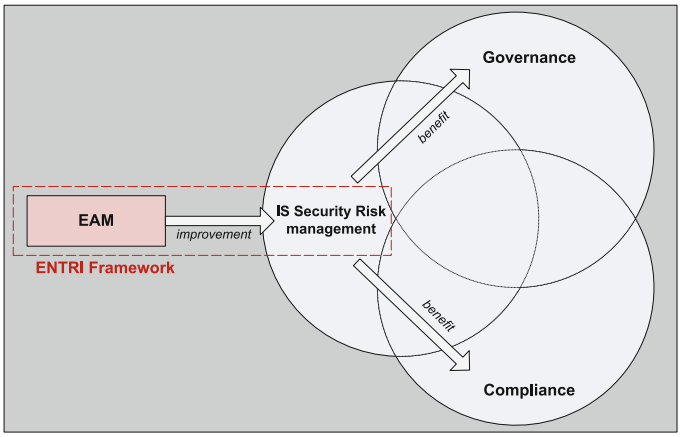

Fig. 2. Research outcome

1. To assess and integrate the conceptual models of EAM and ISSRM domains [contribution 1 = EAM-ISSRM integrated model]
2. To assess and improve the ArchiMate modelling language to support the integrated conceptual model of EAM and ISSRM [contribution 2 = EAM-ISSRM extended language]
3. To analyse the processes supporting both ISSRM and EAM, and to define relevant method fragments/chunks allowing to link both domains at the methodological level [contribution 3 = EAM-ISSRM catalogue of method fragments/chunks]
4. To analyse and position the integrated EAM-ISSRM framework (conceptual model, modelling language and method chunks/fragments), called "ENTRI framework", with regards to GRC models [contribution 4 = GRC-aware ENTRI model, language and method]
5. To implement the designed artefacts on a technological platform called the "ENTRI platform" [contribution 5 = ENTRI platform prototype]

5 Methods and Approach

This research work is especially motivated by the need to fill the gap between GRC and EAM from the IS security perspective. It falls in the frame of Design Science Research (DSR) that tends to design a solution for a specific problem [43]. The research method we want to follow is inspired by the "regulative cycle" approach established by Wieringa [44], that is instantiated to our case in Fig. 3.

Step (1): The motivation of the research work resulted from the observation that ISSRM methods could be improved using EAM, as explained in Sect. 2. This statement is also shared by EBRC (E-Business & Resilience Centre),[3] a leading European datacentre

[3] http://www.ebrc.com.

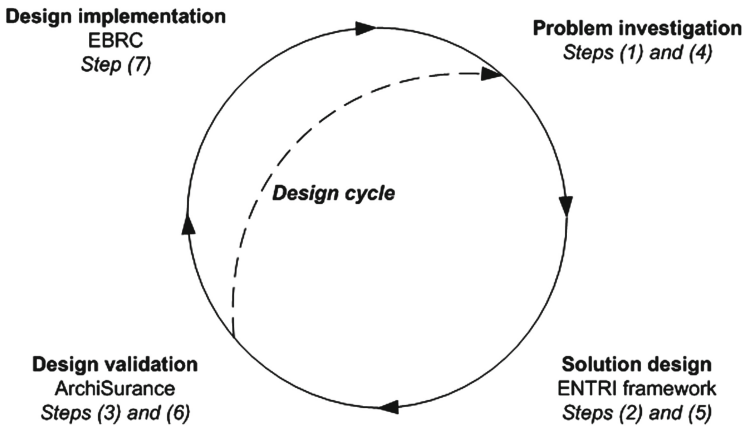

Fig. 3. Research method: A Design Science Research (DSR) approach

operator and our industrial partner, both of us being experienced in running ISSRM methods. EBRC is particularly exposed to governance and compliance problems requiring to perform ISSRM: EBRC holds several certifications (especially the ISO/IEC 27001 certification [45]) and is subject to a set of regulations (financial regulation, tier certification, etc.) many of them involving ISSRM activities having different scopes.

Step (2): In order to achieve our research objectives (Sect. 4), we plan to produce a set of design artefacts called the ENTRI framework and composed of:

- An integrated EAM-ISSRM model
- A integrated modelling language
- A catalogue of method fragments/chunks
- A prototype integrating the preceding results

Step (3): The design validation activity includes the use of the ENTRI framework to run a lab-case study called ArchiSurance [46].

Step (4), (5) and (6): After this first design research iteration, we plan to perform a new design cycle in order to improve our artefacts based on the feedback obtained during the design validation step.

Step (7): Finally, the ENTRI framework will be assessed on a real-world case by EBRC in the frame of improvements of IS security compliance and governance. The ENTRI framework could be compared to their current practices and used in the context of ISO/IEC 27001 certification maintenance [45] and "*Circulaire CSSF 12/544*" [2] compliance for defining an integrated ISSRM system for the company. It is also possible to consider other contractual or regulatory frameworks during this implementation step if additional compliance issues related to our scope apply to EBRC during the design time.

6 Conclusions and Future Work

In this paper, we have described our research background, objectives and agenda in the frame of integrating ISSRM and EAM domains. After having explained the context of our work, we have introduced the current drawbacks of ISSRM approaches: it is generally difficult to model assets, risks and related countermeasures in a meaningful manner, in particular all along the business-to-IT stack. An extensive state-of-the-art has then been established in order to survey the current situation in the field of EAM, its integration with ISSRM and its contextualisation to the emerging GRC field. Our position is that a global framework, encompassing an integrated conceptual model, a modelling language, method(s) and a tool, should be useful to improve the state-of-practice. The expected benefits of such a contribution are numerous: better information security governance, reduction of time and effort dedicated to ISSRM, support in compliance to legal or normative requirements, etc. We plan to demonstrate these benefits through a real-world case-study, with the help of performance indicators.

Regarding current state of the work, the problem investigation step of our research method has been performed and the main observations have been reported in this paper. We are now designing the integrated EAM-ISSRM conceptual model and refining in parallel our coarse-grained research method in a detailed one, taking into account best practices of DSR [44]. Our future works will naturally be focused on following this research method.

Acknowledgments. Thanks to Roel J. Wieringa for his valuable inputs and recommendations about Design Science Methodology. Supported by the National Research Fund, Luxembourg, and financed by the ENTRI project (C14/IS/8329158).

References

1. ILNAS: Technical regulation requirements and measures for certifying Digitisation or Archiving Service Providers (PSDC) (2013). http://www.ilnas.public.lu/fr/confiance-numerique/archivage-electronique/documents-obtention-statut-psdc/index.html
2. CSSF: Circulaire CSSF 12/544 - Optimisation par une approche par les risques de la surveillance exercée sur les “PSF de support” (2012)
3. Official Journal of the European Union: Directive 2009/140/EC of the European Parliament and of the Council of 25 November 2009 (2009)
4. Accenture: Report on the Accenture 2011 Global Risk Management Study (2011). http://www.accenture.com/SiteCollectionDocuments/PDF/Accenture-Global-Risk-Management-Study-2011.pdf
5. Henderson, J.C., Venkatraman, N.: Strategic alignment: leveraging information technology for transforming organizations. IBM Syst. J. **38**, 472–484 (1999)
6. Proper, H.A.: Enterprise architecture: informed steering of enterprises in motion. In: Hammoudi, S., Cordeiro, J., Maciaszek, L.A., Filipe, J. (eds.) ICEIS 2013. LNBIP, vol. 190, pp. 16–34. Springer, Heidelberg (2014)
7. Zachman, J.A.: A framework for information systems architecture. IBM Syst. J. **26**, 276–292 (1987)
8. Saha, P. (ed.): A Systemic Perspective to Managing Complexity with Enterprise Architecture. IGI Global, Hershey (2013)

9. Lankhorst, M.: Enterprise Architecture at Work – Modelling Communication and Analysis. Springer, Heidelberg (2013)
10. 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.) Intentional Perspectives on Information Systems Engineering, pp. 289–306. Springer, Heidelberg (2010)
11. Mayer, N.: Model-based Management of Information System Security Risk (2009)
12. Chowdhury, M.J.M., Matulevičius, R., Sindre, G., Karpati, P.: Aligning mal-activity diagrams and security risk management for security requirements definitions. In: Regnell, B., Damian, D. (eds.) REFSQ 2011. LNCS, vol. 7195, pp. 132–139. Springer, Heidelberg (2012)
13. 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 2008), in Conjunction with the 3rd International Conference of Availability, Reliability and Security (ARES 2008), pp. 1397–1404. IEEE Computer Society (2008)
14. Matulevičius, R., Mayer, N., Mouratidis, H., Martinez, F.H., Heymans, P., Genon, N.: Adapting secure tropos for security risk management in the early phases of information systems development. In: Bellahsène, Z., Léonard, M. (eds.) CAiSE 2008. LNCS, vol. 5074, pp. 541–555. Springer, Heidelberg (2008)
15. Altuhhova, O., Matulevičius, R., Ahmed, N.: Towards definition of secure business processes. In: Bajec, M., Eder, J. (eds.) CAiSE Workshops 2012. LNBIP, vol. 112, pp. 1–15. Springer, Heidelberg (2012)
16. Lapalme, J.: Three schools of thought on enterprise architecture. IT Prof. **14**, 37–43 (2012)
17. Vernadat, F.: Enterprise Modelling: Objectives, Constructs and Ontologies. Presented at the CAiSE Workshops, vol. 3 (2004)
18. Op't Land, M., Proper, H.A., Waage, M., Cloo, J., Steghuis, C.: Enterprise Architecture - Creating Value by Informed Governance. Springer, Heidelberg (2008)
19. Lankhorst, M., Proper, H.A.: Enterprise architecture - towards essential sensemaking. Enterp. Model. Inf. Syst. Archit. **9**(1), 5–21 (2014)
20. Ross, J.W., Weill, P., Robertson, D.C.: Enterprise Architecture As Strategy: Creating a Foundation for Business Execution. Harvard Business School Press, Boston (2006)
21. Greefhorst, D., Proper, H.A.: Architecture Principles - The Cornerstones of Enterprise Architecture. Springer, Heidelberg (2011)
22. Giachetti, R.E.: Design of Enterprise Systems: Theory, Architecture, and Methods. CRC Press, Boca Raton (2010)
23. The Architecture Working Group of the Software Engineering Committee: Recommended Practice for Architectural Description of Software Intensive Systems. IEEE, Piscataway, New Jersey (2000)
24. Anaya, V., Berio, G., Harzallah, M., Heymans, P., Matulevičius, R., Opdahl, A.L., Panetto, H., Verdecho, M.J.: The unified enterprise modelling language—overview and further work. Comput. Ind. **61**, 99–111 (2010)
25. The Open Group: TOGAF Version 9.1. Van Haren Publishing, The Netherlands (2011)
26. The Open Group: ArchiMate 2.0 Specification. Van Haren Publishing, The Netherlands (2012)
27. Saeki, M., Iguchi, K., Wen-yin, K., Shinohara, M.: A meta-model for representing software specification & design methods. In: Proceedings of the IFIP WG8.1 Working Conference on Information System Development Process, pp. 149–166. North-Holland Publishing Co., Amsterdam (1993)

28. Innerhofer-Oberperfler, F., Breu, R.: Using an Enterprise Architecture for IT Risk Management. Presented at the Information Security South Africa 6th Annual Conference (2006)
29. Ertaul, L., Sudarsanam, R.: Security planning using Zachman framework for enterprises. In: Proceedings of EURO mGOV 2005 (2005)
30. 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)
31. 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)
32. 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)
33. OECD: OECD Principles of Corporate Governance 2004. OECD Publishing (2004)
34. Committee on the Financial Aspects of Corporate Governance: Report of the Committee on the Financial Aspects of Corporate Governance. Gee (1992)
35. Managing development: the governance dimension: a discussion paper. World Bank (1991)
36. ISO/IEC 38500: Corporate governance of information technology. International Organization for Standardization, Geneva (2008)
37. COBIT 5: Implementation. ISACA (2012)
38. Racz, N., Weippl, E., Seufert, A.: A frame of reference for research of integrated governance, risk and compliance (GRC). In: De Decker, B., Schaumüller-Bichl, I. (eds.) CMS 2010. LNCS, vol. 6109, pp. 106–117. Springer, Heidelberg (2010)
39. Bonazzi, R., Hussami, L., Pigneur, Y.: Compliance management is becoming a major issue in IS design. In: D'Atri, A., Saccà, D. (eds.) Information Systems: People, Organizations, Institutions, and Technologies, pp. 391–398. Physica-Verlag, Heidelberg (2010)
40. Vicente, P., Mira da Silva, M.: A conceptual model for integrated governance, risk and compliance. In: Mouratidis, H., Rolland, C. (eds.) CAiSE 2011. LNCS, vol. 6741, pp. 199–213. Springer, Heidelberg (2011)
41. Gericke, A., Fill, H.-G., Karagiannis, D., Winter, R.: Situational method engineering for governance, risk and compliance information systems. In: Proceedings of the 4th International Conference on Design Science Research in Information Systems and Technology, pp. 24:1–24:12. ACM, New York (2009)
42. Mirbel, I., Ralyte, J.: Situational method engineering: combining assembly-based and roadmap-driven approaches. Requir. Eng. **11**, 58–78 (2005)
43. Hevner, A.R., March, S.T., Park, J., Ram, S.: Design science in information systems research. MIS Q. **28**, 75–105 (2004)
44. Wieringa, R.J.: Design Science Methodology for Information Systems and Software Engineering. Springer-Verlag, Heidelberg (2014)
45. ISO/IEC 27001: Information technology – Security techniques – Information security management systems – Requirements. International Organization for Standardization, Geneva (2013)
46. Jonkers, H., Band, I., Quartel, D.: The ArchiSurance Case Study. The Open Group (2012)