Deriving and Modeling Compliance Requirements from Legal Audits

Abstract

The overall demand for a stable and reliable financial system prompted the legislators to react by passing regulations preventing further crises. A central part of those regulations is the handling of operational risks in the economy. Financial institutions have to provide more comprehensive capabilities to handle those risks. In order to decrease the vulnerability to risks and since information technology (IT) has become central within the financial system, the induced laws imply consequences to IT systems. Adequate risk management is necessary to meet the legal obligations. Although IT governance and compliance are common parts within IT management, the derivation of concrete measures for existing systems is not trivial. We propose a method to derive concrete legal obligations, classified in requirements, goals and principles. Furthermore we show how existing enterprise models can be enhanced with those demands using the modeling language ArchiMate. We have created several normative models for different areas in IT and discuss one of them, namely "User Authorization Management".

1 Introduction

Information systems enable business operations and support a broad product portfolio throughout different branches, especially in the financial sector. Financial institutions depend more than ever on the services and functionalities provided by information systems. Those encompass the wide spectrum of applications used for interacting with customers, high-speed trading, maintaining business services like insurances or banking accounts, reporting and controlling for the management and many more business operations. Consequently, the centrality of information systems induced that the alignment of business and IT has become a key success factor for companies in general and for financial institutions in particular [1].

Risk management is part of the everyday business of banks and insurances. Evaluating risks, coping with uncertainty and managing changes is part of the business of financial institutions. Nevertheless, politics has formulated additional obligations affecting the institutions in the financial sector, e.g. Basel II, respectively III, Solvency II and the Sarbanes-Oxley Act.

Consequently, the supervision process with regard to the assessment of risk management in banks was tightened. In Germany the scope of risk management is specified through the legal document "minimum requirements for risk management" (MaRisk), defining the statutory requirements for "resources" and "technical-organizational equipment" [2]. The high priority of supervising especially for IT systems is given through the banking act [3, Section 25a.3].

MaRisk has direct impact on the technical-organizational equipment and therefore all technical facilities within a bank. This covers software applications as well as hardware components. In combination with the strengthening of the supervision process implies a new quality of risk management in IT systems. Although risk management is not new in the area of information systems (see [4]), this statutory order has wide reaching consequences. The capability of handling risks in IT systems is due to this not only a primary target of the company itself to ensure the competitiveness and compliance but to fulfill the requirements because violations can cause legal consequences.

MaRisk specifies four different security criteria, namely integrity, availability, authenticity and confidentiality that have to be fulfilled by IT systems [2, Section 7.2]. Although a few general principles like user authorization, or the usage of standards are mentioned MaRisk lacks of detailed requirements and concrete counter measures for risks in the context of IT. This leads to the awkward situation, that responsible persons in companies like enterprise architects, IT architects and software developers do not have concrete specifications what to consider during their implementations, although they are used to have them.

To narrow the gap between the determination of concrete requirements and the interpretation of the legal terminology we propose a method to derive the requirements from audits. We analyze the IT assessments of the German Federal Financial Supervisory Institution (BaFin). Based on the results we can provide normative models according to the requirements. Providing such models in a common IT architecture modeling language is a basis for design and implementation of enterprise architectures, that are compliant and less vulnerable to risks.

The next section discusses major existing approaches that are aiming to implement risk management or to ensure legal compliance in the IT domain, thereby upcoming methodologies like semantic processing of regulatory texts

and smart auditing are mentioned. Section 3 introduces the seven relevant IT areas, which are according to BaFin of great importance and therefore belong to the core of the legal auditing done by the authority. Furthermore, how the modeling process could look like is presented. The concrete modeling of legal requirements and their assignment to existing IT elements is provided in Section 4. Additionally we discuss an annotated and normative model exemplary within the "User Authorization". The paper concludes with a critical remark of the finding and a short outline of upcoming challenges (see Section 5) and a summarizing discussion in Section 6.

2 Related Work

Compliance and governance are parts of enterprise architecture frameworks, like TOGAF and COBIT. TOGAF, as a comprehensive framework for managing enterprise architectures, provides concepts for risk management and governance. Anyway, within the governance process the determination of requirements is not extensively specified but delegated to a role. How the derivation could look like is not discussed in detail [5]. COBIT, an international standard for IT governance, was initially proposed by the Information Systems Audit and Control Association (ISACA) and forms a collection of processes to support governance and compliance. The overall target is to align IT goals and processes with business goals [6]. Detailed risk management is part of the adapted COBIT standard from the IT Governance Institute addressing the Basel II regulation, but again lacks of concrete examples for counter measures by remaining on the high level of business process definitions [7]. Also OCEG advises a structured way of identifying risks and requirements of IT systems by proposing "key business processes", but again concrete implementation details are missing [8]. Although OCEG provides a mapping of those "key business processes" to enterprise areas, the mere existence of processes like "Identification" and "Proactive Actions & Controls" are steps towards risk management but still remain on a high level.

Mayer developed a comprehensive and widely accepted domain model for "Information System Security Risk Management" (ISSRM) [9]. The provided model is "a syntactic and semantic reference" [9, p. 103] for security-oriented modeling languages. Therefore, the ISSRM domain model is a basis for visualizing security aspects in models. The domain model consists in principle of three areas, namely asset-related concepts, risk-related concepts

and risk-treatment related concepts. Mitigate risks, which is a goal of the legal obligations, refers to the latter. Grandry et al. have already introduced a conceptual integration of the ISSRM domain model in the area of enterprise architectures via a concrete modeling language but do not provide a method to derive legal obligations [10]. However, Grandry et al. were able to show the adequateness of the modeling language ArchiMate, which has a strong focus on enterprise architectures, in comprehensive modeling of business objects and risks.

Ensuring compliance via meta-modeling is a common concept in the financial sector. Krdzavac et al. created a metamodel on balance sheets to share knowledge of regulations and to show possibilities of modeling regulations in capital markets [11]. Hereby the advantage of having a model, easy to adapt and transform, lies in the possibility of efficient regulation handling. Carnaghan has shown the importance and different perspectives of audit risk assessment limited to business process models [12]. Strecker et al. argue that modeling is a benefit for auditors since those are confronted with a "remarkable complexity of present days enterprises" [13]. Models support the communication between stakeholders within the audit process. They furthermore argue to enhance technical terminology in modeling languages to achieve suitable models of enterprise architectures.

Motivated by the influence of the Sarbanes-Oxley Act on enterprises Namiri and Stojanovic presented a formal approach to meet the compliance requirements. Thereby they proposed the modeling and implementation of Internal Controls, represented by logical statements, constraining the behavior of business processes. Thereby it is possible to implement a semantic layer ensuring the restriction to requirements, captured as declarative rules and deployed during execution-time on business processes [14]. The question of how those requirements are derived and what content they should provide is not discussed.

Bukhsh and Weigand propose the idea of "Smart Auditing" to meet the upcoming challenges in auditing, like growing risk regulations, compliance requirements and shrinking governmental controls. The proposed "next level auditing" uses smart techniques and a normative model is necessary for compliance checking. A framework supports the creation of IST and SOLL models, which are later on compared using process mining techniques [15].

Additionally to the mentioned concepts, Abi-Lahoud et al. argue for the

usage of "Semantics of Business Vocabulary and Business Rules" (SBVR) to support the machine assistance in processing regulatory texts. Interpretation of regulations into formal representations like the SBVR creates a vocabulary providing practitioners insights into regulatory requirements [16].

In summary, the area of risk assessing audits and supporting the process via concrete models is well analyzed and a variety of literature contributes different aspects. However, prior approaches aim to adapt the existing processes or modeling languages to increase efficiency. Beside of that, we are convinced that it is necessary to analyze how concrete requirements and risks can be determined and prospectively integrated in enterprise architecture models. This leads to an annealing of regulatory policies, auditors and enterprise architects. Within our approach we will focus on supervision of IT architectures in the financial sector.

3 Risk Assessment Areas of IT Architectures In Legal Audits

According to the BaFin there exist several examination areas that are relevant within the determination of risk vulnerability during assessment processes [17]. Those are extensively described in [18] and can be summarized in seven different areas, namely:

1. **IT strategy:** The overall alignment process of business and IT is fundamental, therefore the IT strategy is part of the supervision process.
2. **IT risk management:** Financial institutions have to be aware of operational risks in the IT and provide proper risk management processes.
3. **IT revision:** IT has to be part of the revision process. Paired with control objectives this supports risk management.
4. **IT outsourcing:** Many banks have outsourced services, consequently their vulnerability to risks increases. Adequate countermeasures have to be taken in the context of IT outsourcing.
5. **Emergency management:** Financial institutions need to provide emergency strategies and plans, taking the IT into account.

6. **Application development:** Software applications are important products of IT departments and support the operational business. Awareness of risks is hereby necessary.

7. **User authorization:** Authority abuses and the misuse of software are operational risks to banks. Implementing standards could decrease those and lower the vulnerability to risks.

Covering a wide range of topics within the IT of enterprises these areas should implement a minimal standard of handling operational risks to fulfill the requirements according to MaRisk. The question how representative those areas actually are with respect to risk management, is not part of this work since this would lead to a broad discussion where a variety of additional aspects must be considered. Nevertheless, the BaFin provides comprehensive information on the requirements they have during the assessment.

3.1 Identification of Requirements in the Legal Audit Process

In order to support the audit process, the identification of requirements for enterprise architectures as well as their relations to existing objects is required. The identification of parameters should lead to a normative model representing the minimal requirements of the respective area. Basically this can be done in two ways: analytical and empirical (see Figure 1).

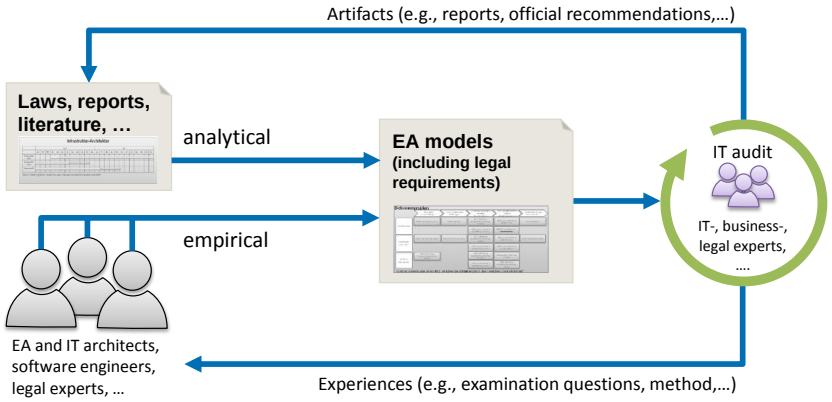

Figure 1: Enhancing EA models with legal requirements as iterative process.

Whereas the analytical way is analyzing existing literature, official publications and reports, the empirical is by deriving requirements from prior

examinations based on experiences during audits. In principle, both methods could yield correct and comprehensive outcomes, influencing existing enterprise architecture models. Experts of the IT domain, like IT and enterprise architects, with experiences to examinations can contribute to the implementation of legal obligation in existing models.

Although it is, due to lack of literature or absence of audit experience, not always possible we argue for a combination where the analytically created models are refined with empirical data and vice versa. Furthermore, the identification and refining is an iterative process, whereas each iteration is a contribution to the improvement of the models. Aware of the fact that the analysis of legal audits can lead to an IT architecture that is conditioned to the requirements of the audit process, we argue that the analysis is a way of proactively understanding drivers for risks and threats and is therefore more than simple conditioning to an examination. Beside of that, legal audits are less rule based but more principle based assessments, preventing the conditioning problem even more. On the contrary, taking the IT assessment into account, ensures the consideration of prior experiences in various companies, which is provided by the auditors. Learning from the auditors is learning from experienced practitioners, e.g., IT-, business- and legal experts.

4 Modeling of Compliance Requirements

The result of analyzing laws, legal regulations and official comments on existing policies can be formulated as concrete requirements associated with existing enterprise architecture models. How requirements should be modeled depends on the specific modeling language. We argue for a classification following the risk treatment-related concepts in the standard ISSRM domain model [9].

Since the compliance requirements aim to reduce the vulnerability to risks, the mapping to the ISSRM domain model, in particular to the risk treatment-related concepts is reasonable (see Table 4). The concepts described by Mayer are intended to "be defined and implemented in order to mitigate possible risks" [9, p. 107]. Hereby the intentions of the ISSRM domain model coincide with the intentions of the MaRisk.

Consequently, we can use an existing modeling language that is common in the IT area, namely ArchiMate. ArchiMate is an open and independent modeling language for enterprise architectures. It provides a notation for de-

ISSRM		**Compliance element**
Control	$\longleftrightarrow$	Goal
Security requirement	$\longleftrightarrow$	IT Principle
Risk treatment	$\longleftrightarrow$	IT Requirement

Table 1: Mapping of compliance requirements of elements for the ISSRM domain model

scribing, analyzing and visualizing relationships amongst enterprise objects (see [19, 20]). ArchiMate allows to create elements on three layers of enterprise architectures, namely business (yellow), application (blue) and technology (green). Beside the core elements (business actor, role, process, function, service, ...) a so-called motivation extension (violet) is implemented [19]. The elements from the motivation extension enable modelers to express concepts like goals, requirements and principles (see Figure 2). This extension provides a way to an enriched architecture model with its motivational components:

1. **Goals:** The general idea of requirements is that they – if fulfilled – lead to "better" systems and the materialization of improvements can be specified in goals. This may be the specified targets of MaRisk, namely integrity, authenticity, availability and authenticity. Therefore goals do not only clarify the intended targets of audits and regulatory policies, but also allow the derivation of further requirements and principles.

2. **Principles:** In order to identify the requirements intentions, principles can be seen as generalizations of requirements. Many different requirements can be used to ensure the implementation of principles, like "historization of changes". Based on those principles it is possible to derive relationships between requirements.

3. **Requirements:** Concrete demands like "software applications must have a version number" that can be assigned to objects and elements are requirements. Those represent the original idea of software requirements.

The model shown in Figure 2 was created using ArchiMate. ArchiMate, enabled us to model the minimal risk requirements specified by BaFin, and furthermore we visualized the motivations and basic ideas that are pursued

by auditors. This was done via the analytical way proposed in Section 3.1 by analyzing the auditors (BaFin) arguments and publications.

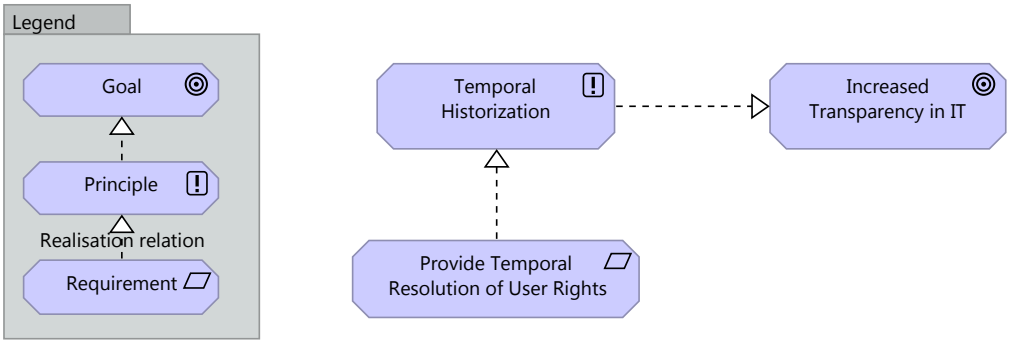

Figure 2: Motivation elements in ArchiMate.

Figure 2 shows the three mentioned elements from the motivation extension. The requirement is at the bottom, the principle at top-left and the goal is placed top-right. The object types is given by the small symbol in the upper right corner of the objects box. The relationship expresses that the requirement "Provide Temporal Resolution of User Rights" is the realization of the more general principle "Temporal Historization". The principle supports the overall goal "Increased Transparency in IT". Figure 2 represents some ideas of the compliance requirements but connected with concrete elements of the enterprise architecture, it provides greater insights to the effect of regulatory policies. Annotating requirements with the motivation extension of ArchiMate is the fundamental idea and doing this in the context of risk management is an intention of the ArchiMate standard (see [20, Section 13.4]).

4.1 An Exemplary Model: User Authorization

The analysis of demands applying to enterprise architectures was done to all mentioned examination areas in Section 3. The identification of the given business elements, and their relations led to seven different models with shared elements. The resulting models represent the requirements for risk management in the respective area, derived from [18].

Figure 3 is an attempt to model the minimal requirements for risk management deduced from official audit literature provided by the BaFin. It is

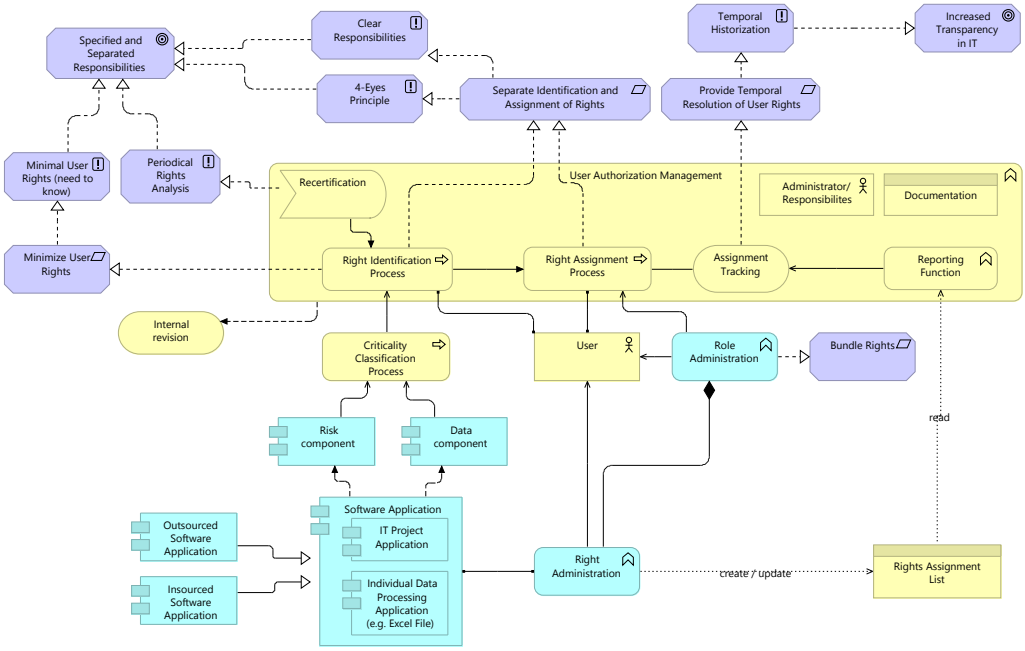

Figure 3: The examination area "User Authorization" derived from official literature modeled in ArchiMate.

not only the visualization of required business objects, it furthermore contains dependencies and relationships as expected from the supervision authority. Enhanced with motivational elements like principles, requirements and goals, it can serve as a base for the preparation of assessments but also for upcoming changes and transformations. The integration of those elements ensures that they are taken into account within future modifications of the enterprise architecture.

The representation of the normative model of the minimal requirements in risk management in the context of user authorization is shown in Figure 3. This model mainly consists of the "User Authorization Management" business function that contains several processes, like "Right Identification" and "Right Assignment", a documentation object, an administrator, a reporting function and an assignment tracking service. The "Right Identification Process" is periodically triggered by the "Recertification" event and the company's "Internal Revision" is aware of the whole function. The "Right Identification Process" uses another process called "Criticality Classification

Process" that operates on the "Risk Component" and "Data Component" of the "Software Application". This is necessary because the application needs to be classified due to its criticality, which is defined by the data an application is processing and the risk an application embodies due to its importance within the business. A "Software Application" itself consists of different kind of applications, like "Insourced Software" or "Outsourced Software". Each software application needs to be associated with a "Right Administration" technology, which is in the easiest way the user account control of the operating system but can also be a built-in service of the application. The BaFin also recommends the usage of roles to bundle user rights. Furthermore a "Reporting Function" is required, that provides access to a valid and actual "Rights Assignment List" and gives an overview of past assignments [18, pp. 282].

4.2 Implicit and Explicit Requirement Modeling

The integration of the requirements can in principal be done using two methods: implicit and explicit. After a requirement is clearly identified, like the separation of the right identification and the right assignment process in Figure 3, the proper business objects can be modeled as two different ArchiMate elements. This is what we call implicit modeling. The necessary requirement does implicitly follow from the given structure. Furthermore a stand-alone requirement is attached to the two processes called "Separate Identification and Assignment of Rights" making the separation explicit. This explicit modeling has the advantage of additional highlighting, although this may lead to over-engineered models and – if overdone – more effort to read and understand the models' content.

Applying the mixture of implicit and explicit modeling users can get an appropriate understanding of the normative implementation of processes and functionalities and therefore an insight in the motivation and intentions of the legal regulations and policies.

4.3 System-wide Modeling of Risks, Goals and Requirements

As mentioned in Section 3 the enterprise architectures of financial institutions are comprehensively assessed, which leads to seven different, but overlapping, examination areas. For each area we visualized the affected business objects and identified the motivation with respect to requirements, principles and

goals. Since we have done this consequently for all areas, we are now no longer limited to the relationships of single objects but can discover system-wide risks, goals and requirements. ArchiMate supports the analysis over different examination areas and is able to identify objects used in different domains and contexts. This unification leads to a repository with system-wide objects. Using those system-wide relationships, holistic analysis of the consequences of goals, principles and requirements in distinct areas of the whole architecture can be performed.

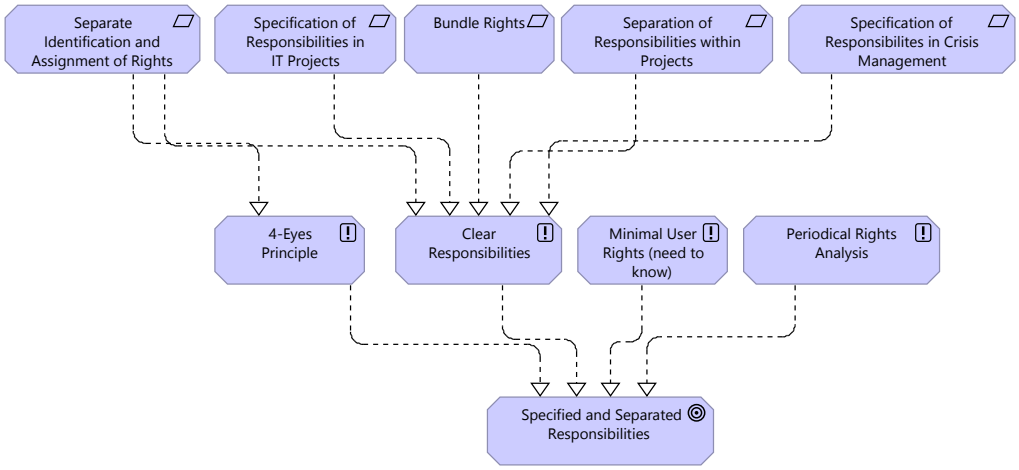

Figure 4: Dependencies emerging from system-wide analysis of relationships.

Figure 4 shows an excerpt of the relationships that emerge while modeling the dependencies and realizations between business elements, requirements, principles and goals. The creation of those views facilitate detailed analysis and collaborative modeling of the enterprise architecture with the effect that the network of relationships and dependencies automatically emerges during the modeling process. The legal requirements do no longer remain abstract but materialize and furthermore can be associated with elements of the company's IT architecture.

5 Critical Reflection & Outlook

The paper presents the rather novel but intuitive approach of assigning legal requirements as well as their objectives to existing models in order to improve the understandability and communicability throughout various changes

in business processes, i.e. maintenance, implementation, transformation etc. Although we did first interviews we are far from providing significant evaluation results, therefore the conduction of further interviews and a comprehensive empirical study is required. In a first feedback, practitioners remarked that although the general idea is coherent, a crucial point will the providing the right level of granularity within the models. Our concept deliberately focused on assigning requirements, principles and goals formulated as free-form comment, i.e. without any predetermined structure.

This paper showed that it is in principle possible to enhance existing enterprise architecture models with legal requirements with the intention to ensure compliance throughout different phases. The next research questions would address the acceptance and usability of those models and our approach in practice. Therefore, the conduction of the aforementioned empirical study is a next step. Additionally, a more structured approach of gathering the requirements using the two mentioned approaches, namely empirically and analytically (see Section 3.1, should be investigated. Hereby guidelines for structuring and formulating may be helpful. The feedback from practitioners as well as of the existing scientific approaches of retrieving essential parts of requirements documents can inspire those guidelines.

6 Conclusion

This paper addresses the risk management in IT-architectures and focuses on the integration of legal requirements. We present a method to extract those requirements from regular occurring IT audits and it's related literature and artifacts. Furthermore, it is necessary to integrate those requirements in the already existing models of the enterprise architecture. Our method supports two approaches that could achieve this: creating normative models representing a minimal standard in a specific area or enhancing existing models with new elements, like requirements, goals and principles. Modeling the requirements can either be implicit or explicit, whereas explicit increases the attention but can lead to over-engineered models requiring additional effort to read and understand. The usage of proper modeling tools support the identification of system-wide dependencies between requirements, goals and principles facilitating further analysis.

The integration of risks and their countermeasures into enterprise architecture models does not only add a new perspective in understanding risks

but supports upcoming changes and transformation. They could ensure continuous awareness of existing risk drivers and principles during the change and transformation process. Additionally, it is a further step towards a common vocabulary of IT-architects in companies and legal regulations in IT governance and compliance.

References

[1] H. Krcmar, *Einführung in das Informationsmanagement*. Berlin and Heidelberg: Springer, 2011.

[2] Federal Financial Supervisory Institution, "Minimum requirements for risk management (MaRisk)," 14.12.2012.

[3] Deutsche Bundesbank, "Banking Act," 2009.

[4] G. Stoneburner, A. Goguen, and A. Feringa, "Risk management guide for information technology systems," *Nist special publication*, vol. 800, no. 30, pp. 800–830, 2002.

[5] The Open Group, *TOGAF Version 9: The Open Group Architecture Framework*. van Haren Publishing, 2009.

[6] ISACA, "COBIT 5: A business framework for the governance and management of enterprise IT," 2012.

[7] IT Governance Institute, "IT Control Objectives for Basel II: The Importance of Governance and Risk Management for Compliance," 2007.

[8] S. L. Mitchell and C. S. Switzer, "GRC Capability Model: Achieving principled performance by integrating the governance, assurance and management of performance, risk and compliance," 2012.

[9] N. Mayer, *Model-based management of information system security risk*. University of Namur, 2009.

[10] E. Grandry, C. Feltus, and E. Dubois, Eds., *Conceptual Integration of Enterprise Architecture Management and Security Risk Management: IEEE International Enterprise Distributed Object Computing Conference Workshops*, 2013.

[11] N. Krdzavac, R. Haque, and T. Butler, "An IFRS compliant balance sheet metamodel," *Federated Conference on Computer Science and Information Systems*, 2012.

[12] C. Carnaghan, "Business process modeling approaches in the context of process level audit risk assessment: An analysis and comparison," *International Journal of Accounting Information Systems*, 2006.

[13] S. Strecker, D. Heise, and U. Frank, "Toward Modeling Constructs for Audit Risk Assessment: Reflections on Internal Controls Modeling," *Modellierung betrieblicher Informationssysteme*, 2010.

[14] K. Namiri and N. Stojanovic, "A model-driven approach for internal controls compliance in business processes," in *Proceedings of the Workshop on Semantic Business Process and Product Lifecycle Management (SBPM 2007), Innsbruck, Austria*, 2007, pp. 40–43.

[15] F. A. Bukhsh and H. Weigand, "Smart Auditing – Innovating Compliance Checking in Customs Control," *IEEE Conference on Business Informatics*, 2013.

[16] E. Abi-Lahoud, T. Butler, D. Chapin, and J. Hall, "Interpreting Regulations with SBVR," *The 7th International Web Rule Symposium: Research Based and Industry Focused, Seattle Metropolitan Area*, 2013.

[17] J. Kokert, "IT-Aufsicht im Bankensektor: Grundlagen," Frankfurt am Main. [Online]. Available: http://tinyurl.com/Bafin-Kokert2013

[18] J. Bretz, *Prüfung IT im Fokus von MaRisk und Bundesbank: Verstärkter IT-Fokus in Sonderprüfungen.* Finanz Colloquium Heidelberg, 2012.

[19] The Open Group, *ArchiMate 2.1 Specification.* The Open Group, 2013.

[20] G. Wierda, *Mastering ArchiMate: A serious introduction to the ArchiMate Enterprise Architecture Modeling Language.* Heerlen: R&A, 2012.