A Metamodel to integrate Control Objectives into Viewpoints for EA Management

Dierk Jugel[1,2], Christian M. Schweda[1], Christina Bauer[1], Jawed Zamani and Alfred Zimmermann[1]

[1] Reutlingen University, Herman Hollerith Zentrum, Böblingen, Germany
{dierk.jugel,christian.schweda}@hhz.de
{christina.bauer,alfred.zimmermann}@reutlingen-university.de
[2] University of Rostock, Rostock, Germany
dierk.jugel@uni-rostock.de

Abstract. Enterprise Governance, Risk and Compliance (GRC) systems are key to managing risks threatening modern enterprises from many different angles. Key constituent to GRC systems is the definition of Controls that are implemented on the different layers of an Enterprise Architecture (EA). As part of the compliance aspect of GRC, the effectiveness of these Controls is assessed and reported to relevant management bodies within the enterprise. In this paper we present a metamodel which links Controls to the affected elements of an EA and supplies a way of expressing associated assessment techniques and results. We complement the metamodel with an expository instantiation in a cockpit for Control compliance applied in an international enterprise in the insurance industry.

Keywords: governance, compliance, control, enterprise architecture, cockpit

1 Introduction

Modern enterprises are faced with threats that originate from different sources. Different varieties of cyber security attacks are on the rise, as recent analyses of the threat landscape show [1]. In addition to cyber security-related threats, environmental factors also pose a risk to modern enterprises operating on a global scale. Architectural risks result from the current set-up of the enterprise and its supporting IT. Finally, legal risks arise from the variety of laws and regulations originating from different sources. Regulations differ in target audiences, with the General Data Privacy Regulation (GDPR) [2] with a broad target and the Versicherungswirtschaftliche Anforderungen an die IT (VAIT – insurance-related requirements for the IT) [3] with a narrow target issued by the German regulator for the financial industry. The Enterprise Governance, Risk and Compliance (GRC) [4] system is established in modern enterprises to diligently handle aforementioned types of risks via cultural, organizational, procedural or technical means, so-called Controls. Objectives of these controls [5] are to

- avoid a risk by changes in the business model;
- reduce the probability of a risk; or to

- limit the impact of a risk.

All types of risks lead to Controls that operationalize the externally imposed rules and regulations. The Controls are implemented into different ‘elements’ of the enterprise, amongst others into business processes as additional checks, into business applications as additional logic, and into the technical infrastructure as additional components. In this sense, the implementation of a control can be seen as attached to the enterprise as a whole or a relevant element within the Enterprise Architecture (EA). In the GRC system the Controls are not only designed, but the enterprise is regularly assessed with respect to compliance with and effectiveness of these Controls. In larger enterprises, these assessments are conducted on different levels: detailed for subject matter experts and aggregated to provide high-level indications for the senior management.

In this paper, we establish an integrated metamodel for Control assessment related to the EA. This metamodel is based on the foundations of GRC, Control modeling, and Control assessments as revisited in Section 2. In Section 3 we present the requirements that lead to the metamodel along ‘user stories’. We instantiate the metamodel (see Section 4) for an exemplary application in the context of an enterprise from the insurance industry in Section 5, and display a prototypic Control Compliance Cockpit supporting different viewpoints on Control assessments. In Section 6 we reflect on the status of the ongoing research and elaborate on the link to risk management.

2 Related Work

COBIT [6] provides a comprehensive framework for governance and management of support for Enterprise IT. In this context, IT-relevant goals of internal and external stakeholders are considered. COBIT provides a process framework complemented by internationally accepted IT process-related requirements. COBIT is based on five basic principles to ensure optimal value of IT. The key principles are the distinction between governance and management, the comprehensive, holistic approach, and the coverage of the entire enterprise. In the process model, governance processes take top priority. These processes set policies and monitor their compliance. The section below deals with management processes which deal with planning, procurement and implementation. These processes are monitored by other management processes and assessed against the given governance guidelines. These monitoring processes are related to performance and compliance, internal control and compliance with external requirements.

The ISO 2700x series considers Controls with the focus on information security. ISO 27001 [7] delineates requirements for the evaluation and treatment of information security risks tailored to the needs of businesses. It provides a framework for developing and maintaining an effective information security management system (ISMS). It will provide IT protection goals in terms of confidentiality, integrity and availability of information. An ISMS in practice consists of the governance view(-point), the risk view and the compliance view. These viewpoints are employed to determine the protective measures considering the different concerns of the enterprise’s stakeholders. The governance perspective relates to the implementation and adherence to objectives, the risk perspective on the identification, assessment and treatment of risks and the compliance perspective on the compliance with regulatory, contractual and legal requirements.

The MEMO approach [8] for enterprise modeling also considers GRC as a key topic. MEMO addresses different stakeholders of and concerns with respect to the enterprise via an integrated set of modeling languages that cover the concerns and are based on one meta-language. MEMO ControlML [9] provides support to stakeholders in the effective and efficient conduct of an assessment of the internal control system and the surrounding organizational action system. The core of ControlML [9] is the Control Objective, which is a desirable condition for achieving an endangered business objective. Control Objectives can be derived from business goals and aggregated. They also determine Reference Objects that are objects to be controlled according the objective. The Reference Object is an abstract concept and represents any concept to describe an enterprise (e.g. business units, applications or technologies). ControlML is complemented by MEMO MetricML [10], which focuses on assessing controls. The Indicator concept described in MEMO MetricML defines the configuration of the indicator as well as the measured values and the date of measurement. The configuration consists of an algorithm for translating attribute's values of Reference Objects into a measurement and the frequency of calculation. The ControlML and MetricML can be combined to cover Control design and Control assessment related in an enterprise model.

Innerhofer et al. [11] provide an overview of how IT-related risks in enterprise architectures can be analyzed and evaluated. This approach provides a detailed process of security management. Because the metamodel of the enterprise architecture does not allow risk analysis and assessment, the metamodel has been enhanced with a security information meta model. This meta-model contains relevant elements that reflect the entire security process. Based on the metatype Model Element, which can accept all elements of any kind of enterprise architecture metamodel, the connection to the enterprise architecture is ensured. There are also elements for the business security objective, security requirement, threat, threat list, incident, security control, and security solution.

Grandy et al. [12] describe the mapping of the metamodel of Information System Security Risks Management (ISSRM) and Enterprise Architecture Modeling Language (EAML) using ArchiMate. They extend EAM to support a security risk-oriented design of an EA. This approach supports the identification of business and information security assets. There is also a proposal to model the treatment of the risk, especially in relation with the value of the risk treatment and with the rationale behind the elements of the architecture. However, there is no support in identifying the threats and vulnerabilities related to the elements of the architecture. It thus provides a mechanism to support the risk model of service companies regarding the security of information systems. The audit on the application of security risk management to service systems is under investigation at the time of this research.

Another approach of Gericke et al. [13] describes a situational method that enables the implementation and integration of a GRC solution. It consists 21 methodological fragments that include the conceptual, strategic, organizational, technical and cultural rollout aspects. It also defines method configurations for different stakeholders. This approach involves only the practice descriptions of the methods and not a true GRC implementation, which requires further research on 'build' and 'evaluate'.

3 Concerns

Insurance companies are exposed to a variety of risks through their core insurance and asset management activities. Including underwriting, operational, strategic but also credit, market, business, liquidity and reputational risks. Internal GRC systems as means to actively govern and manage these risks are therefore prevalent in the insurance industry. We take the perspective of an internationally operating insurance group to derive requirements for our metamodel based on ‘user stories’ reflecting typical stakeholders within the insurance group. The insurance group has a holding structure with over 60 Operating Entities (OEs) represented in more than 70 countries and serving more than 100 million customers. The IT necessary to support the business of the OEs is partly operated by a captive shared service provider, while certain OEs with special situations reserve the right to maintain a local IT. In this context not only efficient and effective but also resilient and above all secure information processing is a key capability for the organization. These demands derived from the company’s business model and regulatory requirements are translated into harmonized Global Architecture and Global Security Standards which are mandatory for all OEs and governed centrally in the holding. These Standards mirror Controls that are designed specifically to purposefully mitigate the identified risks. In this context different stakeholders raise concerns with respect to the GRC system, subsequently documented as ‘user stories’:

Concern 1: Senior management in the holding needs to get an overview of Control compliance and effectiveness throughout the OEs to understand the overall risk exposure of the company and to enter into the planning dialogs with OE senior management resulting in OE-specific target setting.

Concern 2: Subject matter experts in the holding need to understand the status of Control compliance and effectiveness for a specific control area throughout the Group. The experts use this information perform ‘what-if’ analysis to evolve the Controls and get in touch with OE counterparts to derive means of effective implementation.

Concern 3: Senior management of an OE needs to understand the Control compliance and effectiveness in their own OE also compared to the aspiration levels and current levels of assessment as achieved throughout the company. This allows senior management to leverage best-practices from other OEs to improve weak Controls.

Concern 4: Subject matter experts in individual OEs need to understand the defined control objective and their threshold values and see current effects of completed or ongoing measures in order to control the achievement of the specified goals.

4 Solution

The metamodel presented in this section addresses the different concerns and viewpoints on Control assessments as outlined above based on selected approaches from literature – foremost ControlML [9] and MetricML [10] – adapted to the usage context. The metamodel in particular addresses the need for overview on the Group level (see Section 3) by enabling the Control Compliance Cockpit elaborated on in Section 5. The key concepts of the metamodel are introduced in Fig. 1 and subsequently detailed.

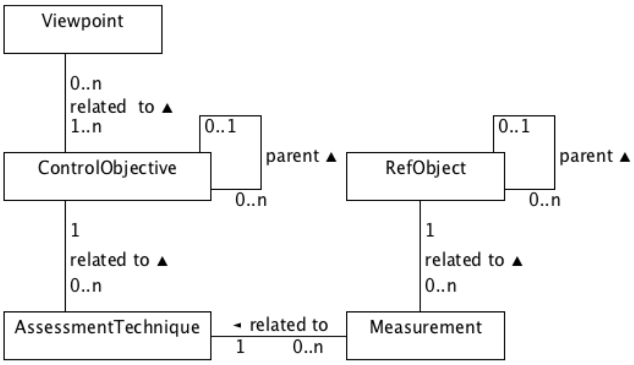

Fig. 1. Metamodel

ControlObjectives – adapted from [9] – represent the functional objectives to control guidelines or regulations. Abstract specifications are operationalized into concrete, architecture-related objectives. *ControlObjectives* define what to control, but not how to assess their effectiveness. The *AssessmentTechnique* – adapted from Indicator as presented in [10] – designates the procedure of assessing and of interpreting the results in terms of 'good' and 'bad'. The Indicator from [10] both represents the assessment process and the result thereof – represented in our case by the concept *Measurement*. The *AssessmentTechnique* also defines necessary calculations, intervals of measurement and thresholds for various effectiveness levels to derive a 'score'. In our setting the scores range from 'very good' to 'very poor' with an extra score for missing values.

In contrast to [9], we assume that *ControlObjectives* are hierarchical and, hence, all of them covered by one *AssessmentTechnique* can be (virtually) grouped to a high-level one. *ControlObjective*s are represented in Viewpoints according to ISO Std. 42010 [14] to facilitate decision making. This aligns with the understanding of the term technique according to the ISO Std. 42010; each *AssessmentTechnique* also defines a way of representing the corresponding *Measurement*s in a viewpoint. We employ the approach outlined in [15] according to which a technique can be applied to a viewpoint in terms of an additional layer adding/changing visual variables of existing symbols. For the Control Compliance Cockpit, we employ color-coding on the different layers.

Each *Measurement* is determined with respect to an element of the EA which is controlled by the corresponding *ControlObjective*. This element of the EA is represented by the concept *RefObject* – adapted from ReferenceObject [9]. Examples of *RefObject*s are OEs or business processes. A *Measurement* is unique for a given combination of *RefObject* and *AssessmentTechnique* at a given point in time. Different time-stamped Measurements may nevertheless exist for different points in time.

Different types of *ControlObjective*s can be distinguished:

- A *DirectControlObjective* targets the EA as a whole.
- A *TypedControlObjective* is dependent on *EAObject* that reflects the facet under consideration. This *EAObject* is an instance of a previously determined type, e.g. ITDomain.

The metamodel reflects this distinction by sub-typing *ControlObjective* (see Fig. 2)

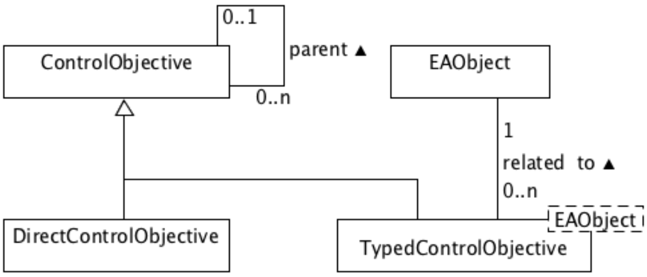

Fig. 2. Specializing *ControlObjective*s

*AssessmentTechnique*s can be distinguished by the way their corresponding *Measurement*s are determined. In particular for grouped high-level *ControlObjective*s no direct assessments may exist, but their results may be derived from more granular *Measurement*s. In line with this we distinguish two types of *AssessmentTechnique*s:

- *DirectAssessmentTechnique*s acquire results by self-assessments or using technical tools for measuring.
- *DerivedAssessmentTechnique*s calculate results based on the results of already performed assessments. For such techniques the individual rules of calculation, e.g. using minimum rule, are specified.

The metamodel reflects this by sub-typing *AssessmentTechnique* (see Fig. 3).

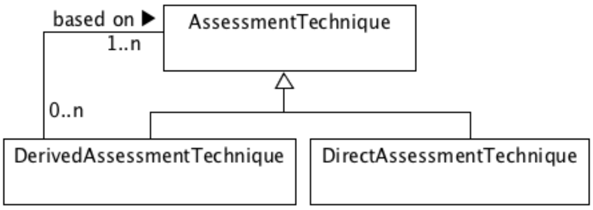

Fig. 3. Specializing *AssessmentTechnique*s

The different kinds of *ControlObjective*s and *AssementsTechnique*s can be combined independently as we show in the exemplary instantiation in Section 5.

5 Control Compliance Cockpit

The metamodel described in Section 4 is the basis for the Control Compliance Cockpit of a company from the insurance industry. This cockpit provides viewpoints giving a comprehensive picture of selected ‘cyber risks’ pertaining to the company – covering cyber security and architecture-related risks. The assessment results with respect to the globally mandated Controls mitigating the ‘cyber risks’ are displayed in a web-based cockpit application, whose main user interface is depicted (in an anonymized manner) in Fig. 4. The user interface displays the company’s OE presence as a world map, identifying ‘Country OEs’ with the corresponding countries and adding non-country-specific OEs (‘Global OEs’) to the passe-partout of the visualization.

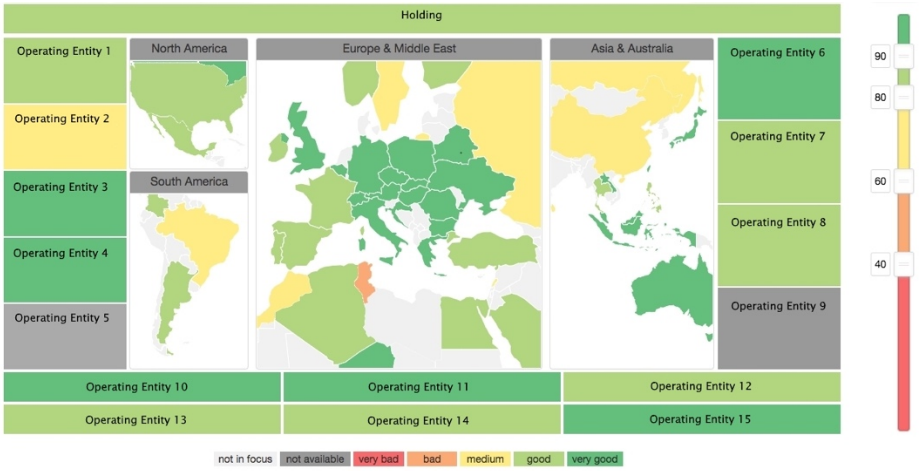

Fig. 4. Control Compliance Cockpit – World Map Viewpoint

The World Map Viewpoint serves as entry point for user interactions. The viewpoint allows to add a layer representing a selected *ControlObjective* via a color-coding. The legend at the bottom of the visualization reflects the scoring system of the respective *AssessmentTechnique* ranging from ‘very good’ (dark green) to ‘very bad’ (red), adding two more colors for ‘not available’ (dark gray) *Measurement*s and ‘not in focus’ (light gray). Latter color indicates countries in which there is no operating OE. The slider on the right side of the visualization directly influences the thresholds specified in the *AssessmentTechnique*. When these thresholds are adapted, the *AssessmentTechnique* recalculates the scoring and the color-coding is adapted. Via this mechanism, subject matter experts are supported in ‘what-if’ analyses.

The Control Compliance Cockpit presents different *ControlObjective*s and *AssessmentTechnique*s, and combinations thereof reflecting the different concerns as introduced in Section 3. Table 1 gives an overview of the combinations employed, precluding their detailed discussion in the following.

Table 1. Examples for combinations of *ControlObjective*s and *AssessmentTechnique*s

	DirectAssessmentTechnique	*DerivedAssessmentTechnique*
DirectControlObjective	ExtV IntV	CSAE
TypedControlObjective	ITAge ITDebt	ArcDebt

The **number of internet-facing vulnerabilities** (ExtV) provides a number of vulnerabilities exposed via internet-facing IP addresses, taking into account the severity of the vulnerability and the time, for which this vulnerability has been exposed. The **number of internal vulnerabilities** (IntV) provides a corresponding assessment for the vulnerabilities being exposed on IP addresses being available from the internal network. The assessment techniques are direct, based on a technical vulnerability scanner.

IT Ageing and IT Debt relate to structuring concepts of the EA, typing the *ControlObjective* to the 'areas', in which the non-compliance is measured. Examples of such structuring elements are different hierarchical types of *ITDomain*s:

- *Infrastructure Domain*s reflect prevalent operating environments for the IT, e.g. data center, workplace and mobile.
- *Technical Domain*s reflect typical use cases for 'commodity' IT, e.g. operating system, database management system and application server.

The **IT Ageing** (ITAge) computes the distribution of IT Assets over the releases of a used technology. A 'left-hanging' distribution is thereby considered an indication for ageing, a 'right-hanging' distribution for actuality of the current IT Asset based with respect to that technology. A technology in turn is assigned to an *ITDomain* reflecting its prevalent operating environment and use case. The **IT Debt** (ITDebt) computes the distribution of IT Assets of Standard to non-standard technologies. The IT Debt is expressed in the amount of money needed to migrate from non-standard technologies to their standard counterparts is considered the corresponding IT Debt.

The aforementioned *AssessmentTechnique*s are direct in terms of Section 4, i.e. their measurements are results of direct assessment. Based on these values the results of following two high-level *AssessmentTechnique*s are derived.

Cyber Security Attack Exposure (CSAE) provides a cumulated view on the exposure to cyber security related attacks resulting from organizational, procedural and technical vulnerabilities that can potentially be exploited by an attacker. The value of an OE's measurement is derived from the assessments of constituting control objectives. The score of the measurement is determined by applying a minimum operation to the scores of the constituting *AssessmentTechnique*s, reflecting a worst-case assumption with respect to exposure.

The **Architectural Debt** (ArcDebt) provides a cumulated view on potential costs and disadvantages that result from non-compliance to Global Architecture Standards and missing investments into IT rejuvenation. The value of the OE's measurement is derived from the assessments of constituting control objectives. The Architectural Debt for an *ITDomain* combines operating environments (as the top-level) and use cases (at the child-level), e.g. 'operating system on workplace'. The value is determined by applying a summation over the values of the constituting *AssessmentTechnique*s.

The **number of internet-facing vulnerabilities**, the **number of internal vulnerabilities** and the **Cyber Security Attack Exposure** all consider the OE as a whole, making them *DirectControlObjective*s in terms of Section 4. The **Architectural Debt** and its constituting **IT Ageing** and **IT Debt** are conversely *TypedControlObjective*s bound to the EA concepts *ITDomain* and *Technology* and can be assessed for any instance of these concepts, e.g. the aforementioned *ITDomain* 'operating system on workplace'.

Aforementioned *ControlObjective*s and *AssessmentTechnique*s can be described via a model (see Fig. 5) instantiating the metamodel from Section 4. The *TypedControlObjective*s employed reflect their 'binding' to *ITDomain* and *Technology*, as discussed above, via a parameterization with the corresponding types. This allows to leverage for the actual instances of **Architectural Debt**, **IT Ageing** and **IT Debt** the existing relationships between the related *Technology* and *ITDomain* instances from the EA model.

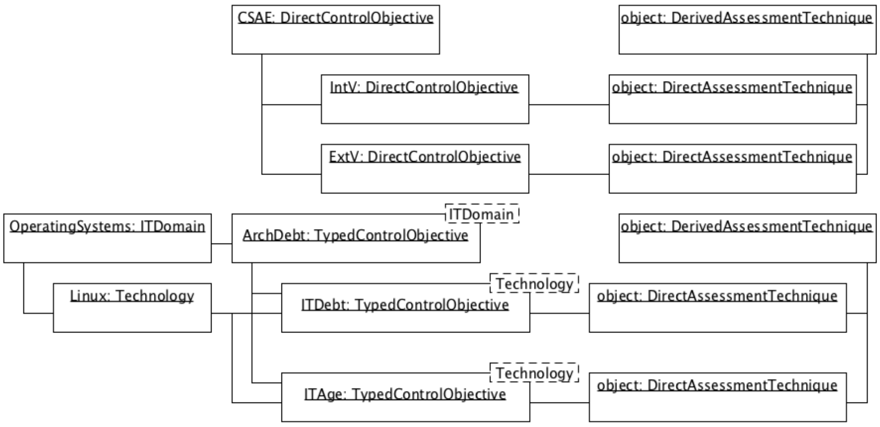
CSAE: DirectControlObjective
object: DerivedAssessmentTechnique
IntV: DirectControlObjective
object: DirectAssessmentTechnique
ExtV: DirectControlObjective
object: DirectAssessmentTechnique
ITDomain
OperatingSystems: ITDomain
ArchDebt: TypedControlObjective
object: DerivedAssessmentTechnique
Technology
Linux: Technology
ITDebt: TypedControlObjective
object: DirectAssessmentTechnique
Technology
ITAge: TypedControlObjective
object: DirectAssessmentTechnique

Fig. 5. Exemplary instantiation of *ControlObjective*s and *AssessmentTechnique*s

6 Conclusion

In this paper, we addressed the relationship between Governance, Risk and Compliance (GRC) and Enterprise Architecture (EA). We presented typical concerns from a practical setting in Section 3 and used them to derive a metamodel (in Section 5) that is capable of integrating Control Objectives with the structuring concepts of an EA. This metamodel accounts for the relevant pre-work, revisited in Section 2 in particular the work around ControlML [9] and MetricML [10]. The exemplary instantiation of the metamodel in the context of the Control Compliance Cockpit piloted in an insurance company (cf. Section 5) shows applicability and versatility of the developed concepts.

The Control Compliance Cockpit with the layers that are built on the *AssessmentTechnique*s provides evidence that the *DerivedAssessmentTechnique* very well fits the need of company stakeholders for aggregated measurements with respect to *ControlObjective*s. The use of *TypedControlObjective*s in turn showed that a parameterization of control assessments by respective structuring concepts of the EA fits the needs of subject matter experts within the company.

In type-theory, a *TypedControlObjective* is considered a 'template class' with one formal parameter bound to a concept from the EA metamodel. Further research is needed to show if and how relationships between concepts from the EA metamodel systematically translate to relationships between *AssessmentTechnique*s. Having multiple formal parameters for *TypedControlObjective*s might prove of use in this context.

References

1. European Union Agency for Network & Information Security (ENISA): ENISA Threat Landscape Report 2017. (2017).
2. European Parliament: Regulation 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data. Off. J. Eur. Union. L119, 1–88 (2016).
3. Bundesanstalt für Finanzdienstleistungsaufsicht (BaFIN): Versicherungswirtschaftliche Anforderungen an die IT. (2018).
4. Proctor, P.E., Wheeler, J.A., Pratap, K.: Definition: Governance, Risk and Compliance. (2015).
5. Bundesamt für die Sicherheit in der Informationstechnik: BSI Standard 200-3: Risk Analysis based on IT-Grundschutz – Version 1.0. (2017).
6. ISACA: COBIT - A Business Framework for the Governance and Management of Enterprise IT. (2013).
7. International Organization Of Standardization: ISO/IEC 27001: Information technology - Security techniques - Information security management systems - Requirements (2nd edition). (2013).
8. Frank, U.: The MEMO meta modelling language (MML) and language architecture (2nd edition). , Duisburg-Essen (2011).
9. Heise, D., Strecker, S., Frank, U.: ControlML: A domain-specific modeling language in support of assessing internal controls and the internal control system. Int. J. Account. Inf. Syst. 15, 224–245 (2014).
10. Strecker, S., Frank, U., Heise, D., Kattenstroth, H.: MetricM: a modeling method in support of the reflective design and use of performance measurement systems. Inf. Syst. E-bus. Manag. 10, 241–276 (2012).
11. Innerhofer-Oberperfler, F., Breu, R.: Using an Enterprise Architecture for IT Risk Management. In: Proceedings of the ISSA 2006 from Insight to Foresight Conference. pp. 1–12 (2006).
12. Grandry, E., Feltus, C., Dubois, E.: Conceptual Integration of Enterprise Architecture Management and Security Risk Management. In: 2013 17th IEEE International Enterprise Distributed Object Computing Conference Workshops. pp. 114–123. IEEE (2013).
13. 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 - DESRIST ’09. p. 1 (2009).
14. International Organization Of Standardization: ISO/IEC/IEEE 42010:2011 - Systems and software engineering -- Architecture description. (2011).
15. Jugel, D.: Modeling Interactive Enterprise Architecture Visualizations: An Extended Architecture Description (submitted paper). Complex Syst. Informatics Model. Q. (2018).