RMDM – Further Verification of the Conceptual ICT Risk-Meta-Data-Model

Verified with the underlying Risk Models of COBIT for Risk and COSO ERM 2017

Martin Latzenhofer [1] [2]
[1] Center for Digital Safety & Security
Austrian Institute of Technology
Vienna, Austria
email: martin.latzenhofer@ait.ac.at

Gerald Quirchmayr [2]
[2] Multimedia Information Systems Research Group
Faculty of Computer Science, University of Vienna
Vienna, Austria
email: gerald.quirchmayr@univie.ac.at

Abstract— **The aim of this article is to introduce an approach that integrates the different models and methods currently applied for risk management in information and communication technologies (ICT). These different risk management approaches are usually bound to the organization where they are applied, thus staying quite specific for a given setting. Consequently, there is no possibility to compare or reuse risk management structures because they are individual solutions. In order to establish a common basis for working with different underlying risk models, a metamodeling approach from the area of disaster recovery is used. This contribution describes a comprehensive mapping of information artefacts from both the COBIT for Risk and the COSO Enterprise Risk Management (ERM) framework in its new 2017 version which are then lifted to the meta-level of the proposed ICT risk-meta-data-model in order to be able to work with them in a consolidated way. Through this mapping process, all information artefacts are extracted, consolidated and harmonized to minimize the number of relevant objects. It has turned out that both the list of consolidated objects and the derived describing attributes can in general be incorporated into the proposed ICT risk-meta-data-model (RMDM). The results show that it is worth examining a data-structure-oriented approach to develop both a model and a data structure for further framework-independent processing.**

Keywords-information and communication technology risk management; ICT risk-meta-data-model; COBIT for Risk; COSO ERM 2017; metamodeling; UML.

I. INTRODUCTION

In literature and in practice, many different risk management approaches and models can be found for the area of information and communication technology (ICT) systems. Even within the field of ICT, these approaches and models are tailored quite narrowly to specific areas and are typically restricted to one single organization. Therefore, the information on risk management is usually not comparable and transferrable between different organizations. This means that the risk model, the established risk management method, the concrete process implementation, the required input data and the resulting outcome have to be adapted to the current requirements of an organization every time the risk management process is set up. This often leads to high efforts for an organization or a company because they have to initialize and re-establish the risk management frameworks and related processes each time. It is evident that these parameters result in a smaller degree of reusability of a given risk management process and less comparability of the information obtained from it.

When interpreting this problem as a pure ICT issue, an explicit ICT solution is required. This leads to the main research question of this paper, i.e., whether it is possible to develop a common risk management model, which is flexible enough to be applicable in different fields of the ICT area as well as among different organizations. To achieve that, it is crucial to define a suitable level of modeling. Therefore, the goal of the introduced approach is to design a meta-model for ICT risk management. By integrating different existing ICT risk management models, which are suitable for various fields of application into a meta-model, a generic data structure that focuses on common aspects of these models can be developed. This umbrella model simply obtains data from the underlying specialized models that have been defined by different frameworks. In this work, the first mapping was performed with the risk model included in COBIT for Risk. Subsequently, the same transformation method was applied to another risk model that forms part of the COSO ERM 2017 version. The approach introduced in this article postulates a superordinate meta-model for ICT risk management and represents it as a data model, which is expressed as a UML class diagram. The iterative performance of the mapping strengthens the first result of the meta-model and ensures the detailed design of classes, attributes, and methods. Considering the application of ICT risk management in practice, the state-of-the-art frameworks are well-established in the daily business of organizations. Consequently, it is not realistic to replace them by a new, universally valid model. The ICT risk-meta-data-model approach introduced here firstly establishes a common data base of risk information gathered by different risk management frameworks, secondly makes data retrieved from different sources comparable, and thirdly verifies its practical applicability by describing real-life use cases, shown as an instantiation of the ICT risk-meta-data-model.

The main goal is to specify the meta-model as a substantial data model. Using such a precise data model, the meta-model is directly applicable to real-life scenarios and enables the implementation of a dedicated ICT application or

data structure. The data model is directly applicable for ICT tasks, provides a concrete ICT data structure where risk information can be stored, and is a fundamental (data) basis for ICT risk management applications.

The authors' conference paper for SECURWARE 2017 discussed a first comprehensive mapping of a concrete risk model – provided by COBIT for Risk – to the ICT risk-meta-data-model [1]. This present journal paper now integrates a second risk model from COSO ERM 2017 into the proposed RMDM, which has led to further adjustments and thus a more sustainable structure of the RMDM. The originating idea of the conceptual ICT risk-meta-data-model was first introduced as a draft proposal at DACH Security 2016, in Klagenfurt, Austria [2].

This article is divided into five main sections. Following this introduction, Section II starts with a short introduction of the common risk management framework COBIT for Risk, which was selected for the first mapping of risk models to the meta-model level. It discusses the processes of COBIT for Risk which are relevant for managing risk in detail. Section II continues to shortly introduce the COSO ERM 2017 framework as the second risk model that has been mapped. Subsequently, it describes the fundamentals of the applied metamodeling approach and concludes with discussing related work. In Section III, the conceptual data model RMDM, described in Unified Modeling Language (UML) is introduced. The version of the RMDM that is presented in this work represents the current state of the model after the two mappings mentioned above have been performed. Section IV firstly discusses the mapping of the information artefacts, input and output components of COBIT for Risk, which are the core of the derived risk model, the objects of the proposed ICT risk-meta-data-model (RMDM) and the results of the mapping in detail. In line with this approach, the second part of Section IV documents the mapping of COSO ERM 2017 and the respective findings, which resulted in a slight refinement of the UML classes. The general objective of this section is to apply the postulated meta-model by modeling an instance of two concrete risk models. Both mappings represent an analysis of whether modeling at the meta level works in general. The concluding Section V outlines the results and proposes further research that is needed to refine the ICT risk-meta-data-model (RMDM).

II. FUNDAMENTALS

Typically, organizations have a continuous need to manage the risks in their business environment. Such a need due to extrinsical factors is often motivated by legal requirements. Organizations have to ensure compliance with regulations, especially relating to finance and public accounting. Therefore, the responsible person implements risk management – in this case limited to the ICT area – by doing research and building upon already existing risk management structures. Special risk management frameworks that are applicable to ICT, e.g., International Organization for Standardization (ISO) 31000 [3], National Institute of Standards and Technology (NIST) Special Publication (SP) 800-30/-37/-39 [4] [5] [6], Committee of Sponsoring Organizations of the Treadway Commission (COSO) Enterprise Risk Management (ERM) [7], Management of Risk [8] or COBIT for Risk [9], have proven to be effective within one single organization. These frameworks set up a baseline in an organization when it comes to implementing risk management structures. This usually generates isolated solutions. The different risk management frameworks are characterized by relatively similar objects and terms but very different artefacts, which cannot be related, compared, or summarized. One important issue is to harmonize the semantic differences between the various risk management frameworks, and even within one single framework.

A. COBIT for Risk

COBIT for Risk [9] is a special publication edited by Information Systems Audit and Control Association (ISACA, since 2008 the acronym itself is used as a brand name) [10] and is entirely based on Control Objectives for Information and Related Technology (COBIT, since version 5 only the acronym itself is used as a brand name) 5.0 [11], a framework for governance and management of Enterprise ICT, especially for the interaction between ICT and classic business objectives. COBIT for Risk is a comprehensive guide for risk professionals. It elaborates the driving aspects for risk management in COBIT – principles and enablers – and extends the framework with risk scenarios. Furthermore, it provides suggestions for appropriate response measures using a combination of enablers. It has – similar to ISO 31000 [3] – a two-tier approach: the risk management perspective puts the high-level principles into practice and the risk function view seeks to identify relevant COBIT processes, which support the risk management, as depicted in Figure 1. In this figure, the two core risk processes are shown in light blue, the other twelve key supporting processes are colored in dark red.

The COBIT for Risk framework was chosen as a first candidate for the intended mapping because of its good balance between general applicability for risk management topics and very specific statements in form of concrete control objectives for risk management. It definitely provides much more topic-oriented reference-points than standard COBIT. The framework is clearly structured and its description is not too narrative. A highly narrative framework might increase the effort for identifying class objects. In summary, all these characteristics were considered to be good prerequisites for the practical mapping work. Other frameworks, e.g., ISO 31000 [3], might be too generic in order to derive substantial class objects to a sufficient extent or, e.g., NIST [4] [5] [6], is too text-heavy for an efficient proof of concept. Consequently, all the other frameworks are rather suitable for verifying the ICT risk-meta-data-model in a more advanced state of development.

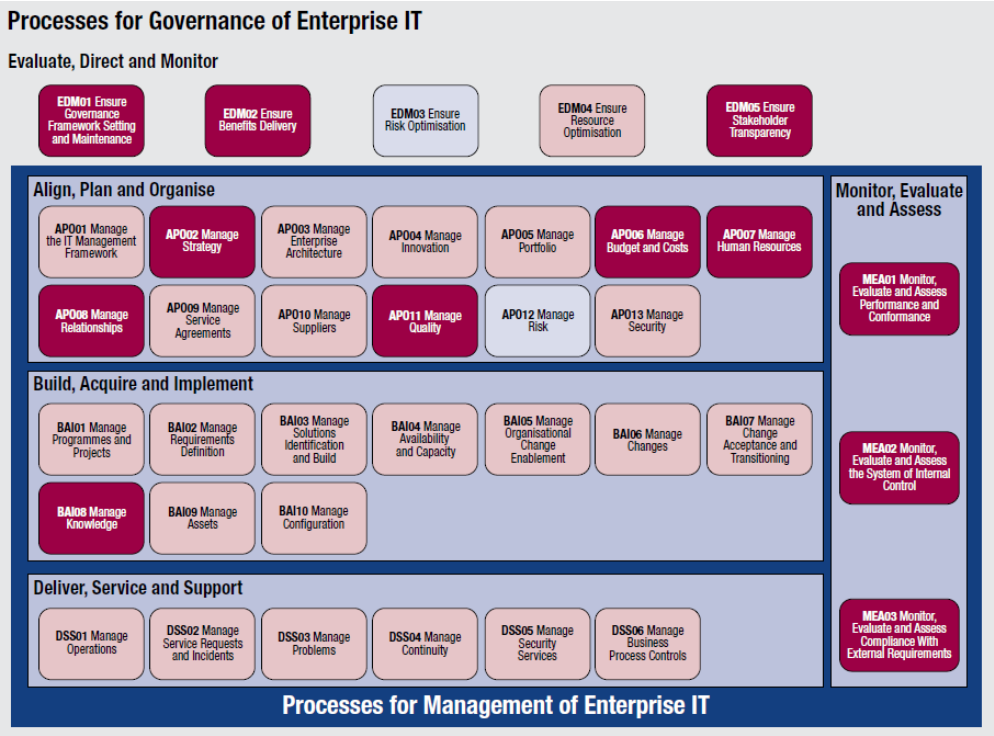

Figure 1. Supporting COBIT processes for the risk function [9, p. 35]

B. COSO ERM 2017

The first version of the "Enterprise Risk Management – Integrated Framework" (ERM) [12] was published by the Committee of Sponsoring Organizations of the Treadway Commission (COSO) [13] in 2004 and was an extension of their first "Internal Control – Integrated Framework" publication from 1992 [14]. In the middle of 2017, COSO fundamentally revised the comprehensive ERM framework in cooperation with PricewaterhouseCoopers (PwC) [15] to address the raising complexity of risk in the business environment. The ERM framework aims at providing guidance to managers on how to handle different kind of risks in an appropriate way. The main objective of this framework is to offer managers specific methods and techniques for managing risks in their organization and to provide them with different use cases.

In general, the COSO ERM 2017 framework emphasizes the relationship of risk management activities with the organization's strategy, business objectives and current performance in order to raise the value that is derived from the organization's mission, vision, and core values. This requires consistent risk management activities at all levels of the enterprise. The main objective is to establish a balance between risk and performance by developing a coherent risk profile based on an appropriate risk appetite that depends on the individual situation of the organization on the market. Typically, the performance targets and risks vary to a certain degree, which is referred to as tolerance in performance and risk capacity of the organization. Consequently, the organization seeks to reach the best possible performance within the given restrictions over time.

The framework itself is a set of 20 principles that are categorized by five interrelated components, which are illustrated in Figure 2. The first component "Governance & Culture" addresses the setup of the organization, which includes the organizational structure, the definition of core values and of behavioral expectations, and the organization's reliability and accountability. The second component "Strategy & Objective Setting" defines input requirements for the risk management in the organization: e.g., business context, risk appetite, alternative strategies and business objectives. Once the risk management framework has been set up, the organization can conduct the operational risk management process, which is described in the component "Performance". In this process, the risk manager identifies, assesses and prioritizes risks, implements risk responses and develops an oversight portfolio view of all risks. In the "Review & Revision" component, the risk manager reviews the changes in risk and performance. The last component, "Information, Communication & Reporting", deals with communication and reporting issues.

Although this framework follows a typical top-down approach, it differentiates between the different levels in an organization – i.e., governance and strategic level (the first two components) and operational level (especially the third component). However, it also addresses the guiding processes for reviewing the risks in the fourth and communication in the fifth component; as it is also done in

Figure 2. COSO ERM 2017 Risk Management Components and Principles [15, p. 21, Fig. 5.1 / pp. 22, Fig. 5.2]

ISO 31000, COBIT for Risk, and the relevant NIST special publications. The 20 principles provide a good set of key principles which management has to follow in order to establish mature risk management processes in the organization. COSO ERM 2017 discusses the problem of cascading risks, continuous changes of risks and the required adjustments of the risk profiles and established responses, and it covers cost implications.

The COSO ERM 2017 framework was mainly chosen as the second candidate for the mapping because of its dense content and because its narrative description is similar to COBIT for Risk. Additionally, the new version of COSO ERM from June 2017 provides an up-to-date perspective on the current business complexity and risk management measures. Consequently, COSO ERM 2017 represents a suitable framework for further verifying and developing the RMDM after the first verification by the risk model of COBIT for Risk.

C. Metamodeling Approach

The semantic meaning of a risk model must be transferred to the meta-level. A formal, scientific approach to build a consistent umbrella is missing. The meta-modeling process helps to create a common basis for standardization. The instantiation procedure of the meta-model down to the distinct risk management framework provides rules for transferring data from a concrete model up to the meta-model, and is in that way working as a normalization process. The first advantage of representing the risk-meta-model as data model is the immanent design of a structured data management based on a semantic model. It must be verified whether the general concepts can be divided from content-specific aspects in such a way that the interaction between meta- and model-level still remains efficient. The data model works as a structure model and holds static information. The risk management process and corresponding workflows change this data dynamically, providing a data model for the whole risk management life cycle. However, this article focuses on the verification of the basic content and on whether the data model can process the information. In addition, the meta-model approach for standardizing risk management information can be implicitly verified by setting up the data model, at least for those risk models which have been analyzed earlier. Certainly, it is no evidence for its comprehensiveness that all existing risk models still fit in the proposed meta-model. In fact, some models might be unsuitable for mapping. However, re-performing the transformation process for a specific number of widely accepted risk frameworks ensures that the meta-model is sufficiently applicable for risk management tasks in organizations.

In the context of a metamodeling hierarchy according to Karagiannis and Kühn [16] (cf., Figure 3), the ICT risk-meta-data-model is situated on Level 2 – Metamodel, described by the Metamodeling Language UML. The selected risk management framework, e.g., COBIT for Risk [9], corresponds to Model on Level 1. It is described by means of the published framework, here in a semi-narrative way. The underlying Original itself can in fact be referred to as Level 0, and represents the organization's risk management structure facing a concrete risk situation. On the top of the hierarchy, the Meta²-Model on Level 3 defines the structural elements of the general UML class diagram. The Meta²-Modeling Language can be understood as the modeling language UML used to describe the ICT risk-meta-data-model.

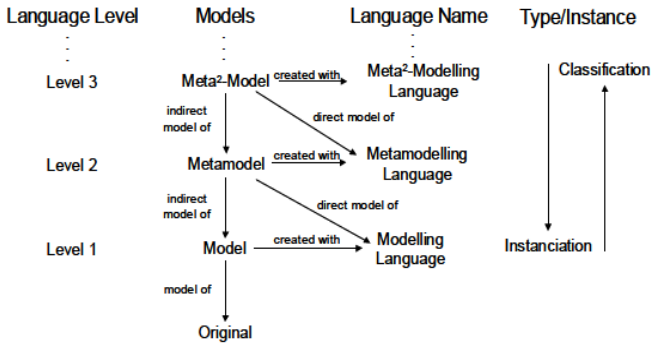

Figure 3. Metamodeling hierarchy [16]

D. Related Work

A lot of academic work has been published on selecting the best risk model or the most promising method to identify and assess ICT risks. Literature research on the general subject of risk management modeling has shown that there are certain common issues that are typically encountered. One issue is the complex application field which the conventional risk management models cannot satisfactorily cope with. Typical examples for difficulties are cascading effects of risks, a broad diversity of possible risks not being able to cover the complete risk landscape or even a high degree of uncertainty. Some recent works deal with ICT risks in established domains which remain hard to manage, e.g., outsourcing, project management, software development; relatively novel innovative environments like cloud computing, internet of things (IoT) with still diffuse risk implications; or previously independent and even stand-alone domains which are now merging, e.g., safety and security or cyber-physical systems (CPS) in relation to ICT. It should be noted that risk management structures and measures, including many different and widely accepted models, have already been established in organizations. However, they tend to struggle with different types of models because in many cases none of them fits their individual requirements completely.

At least four different approaches can be identified. The first category of scientific approaches the proposal of "yet another new/integrated/simplified/formally structured model". The following citations refer to representative examples for this category that were found during the literature research and are definitely not exhaustive: e.g., for cloud computing risks [17], enterprise risk [18], outsourcing risks [19], or even general information security risks [20], which may be appropriate for the very specific situations and circumstances for which these models have been developed for. However, this interpretation generates even more models and leads to the fact that models are not universally applicable. A second approach of the scientific community is to apply combinations of different already existing models or methods to get a more accurate and/or comprehensive result. A representative example for outsourcing can be found in [21], for project management in [22], or risk mitigation decisions in [23]. Thirdly, digging a bit further into the inherent structure of risk models, there are other remarkable approaches which link different methodological approaches together, e.g., simulation, empirical studies and/or modeling approaches [24] [25]. The fourth strategy – which seems to be the most promising approach for the present task – is to generalize the models and to transfer them to a superordinate meta-level. Obviously, meta-modeling is an interesting approach when all the challenges discussed in the previous paragraph arise: firstly, a complex and diverse application domain (e.g., ICT risk management) which cannot be analyzed satisfactorily with one single model among the variety of different and already applied structural frameworks (e.g., all the widely accepted risk management frameworks like ISO 31000, NIST, COSO, COBIT for Risk). However, the risk models do not fit in every aspect (e.g., strategic or operational, business or technical risks) and sometimes even combinations of different approaches (e.g., modeling or simulation, quantitative or semi-quantitative if possible versus qualitative approaches) lead to different and partially contradictory results. In fact, meta-modeling promises good results when a methodological superstructure does not exist. Representative contributions for this approach which address the inherent complexity of specific domains can be identified for e.g., safety and security [26], big data [27], cyber-physical environments [28], or even information system security risk management [29].

The approach introduced in this article is explicitly inspired by similar work in the field of disaster recovery [30] [31], which introduced a meta-model integrating data from different natural disaster scenarios. Othman and Beydoun have implemented a data model in order to store data relevant to disaster recovery and have conducted a proof of concept for two natural disaster incidents of recent history, the Christchurch earthquake and Fukushima nuclear incident [31]. In this article, their approach is shifted into the ICT risk management domain while verifying whether it is a sustainable method for risk management.

III. ICT Risk-Meta-Data-Model (RMDM)

This section introduces the proposed ICT risk-meta-data-model and its current status of development up to now, followed by a discussion about the main components.

A. General Requirements

One of the main objectives of the conceptual ICT risk-meta-data-model is to record key information of any underlying risk model in a way that it can be compared, consolidated, merged and subsequently analyzed from an abstract meta-perspective. This approach ensures that risk management models that have already been implemented in organizations in practice continue to be used, at least the most commonly applied frameworks. Furthermore, this abstraction step reduces the information risk managers work with to the really essential requirements needed to establish the risk management framework and to perform the risk management process. This transformation from the risk model to the more abstract and general meta-level must follow specific rules and definitely causes some information loss. To succeed it is necessary to strike a viable balance between the appropriate level of detail of the information content – by selecting only the key data, combining it

semantically correct and transferring it to the meta-level – and the complexity level of the risk-meta-data-model. The authors assume that an adequate level of abstraction is reached when three to four structurally different risk models can be consistently represented as instances of the ICT risk-meta-data-model. This iterative refinement of the risk-meta-data-model through the analysis of different underlying risk models enhances its sustainability and robustness for practical application. The major advantage of formulating the ICT risk-meta-data-model as an ICT data model is that this allows organizations and companies to apply it in practice. By depicting the meta-model as unified modeling language (UML) classes diagram the modeler can immediately generate the corresponding data structure, implementing a demonstrator, which can serve as a proof of concept. Consequently, the ICT risk-meta-data-model itself constitutes an ICT application that can be applied in practice. In other words, the ICT problem to merge data from different risk models requires an ICT solution, which can immediately be applied by IT means.

The first draft of the ICT risk-meta-data-model was developed based on literature research on different risk management frameworks, which all propagate distinct risk models but use the same or similar terms. The literature research also indicated that there is a need to reflect on the exact meaning of the used terms, even if they seem to be identical. A feasible mapping of the concepts used in different risk models is a prerequisite for successfully raising the key information of the risk model up to the meta-level. This requires the definition of consistent concepts on the meta-level in order to prevent overlapping of concepts and resulting misinterpretations. However, it depends on the specific framework whether the risk model can be derived directly from the publications. ISO 31000 [3], for example, is formulated in a generic way, thus leaving room for interpretation. COBIT for Risk [9], does in contrast provide very specific control objectives for the key and supporting processes on a more detailed level. This characteristic was the main reason for selecting COBIT for Risk for the first mapping of a risk model to the ICT risk-meta-data-model.

The conceptual model aims at reflecting both the fundamental framework establishment and the operative risk management process that covers the risk management lifecycle. This dual perspective is a key feature of many frameworks and easily visible in, e.g., ISO 31000 [3], NIST [4] [5] [6], or even COBIT for Risk [9] or COSO ERM 2017 [15]. A core aspect was to identify appropriate objects, which represent the focus points within the risk management structure. These objects are further described by dedicated attributes, which are the variables for storing the relevant risk management information. These attributes can be changed, modified, extended, and adapted by specific methods. By setting up this data structure it is possible to transfer all relevant risk management data from the origin model up to the ICT risk-meta-data-model. A very first draft of the modeling was already introduced in [2]. This article included a first draft of the ICT risk-meta-data-model and a possible approach for a proof of concept by applying COBIT for Risk as the underlying risk model. The first version of the ICT risk-meta-data-model was the result of a creative process. This process followed the life cycle of risk management: starting with the identification of risk factors, followed by the analysis of the resulting risk by linking it to the current challenges that the organization has to cope with, and finally the evaluation of the risk. Furthermore, the data-model may represent the monitoring of established treatment activities. As a consequence, the data model fulfills the essential requirements of the risk management process as suggested in [3]. The next step was to perform a precise mapping of information artefacts propagated by COBIT for Risk [9] as described in Section IV A and B. The logical next step was to repeat the mapping with another fully applicable risk management framework. The selected COSO ERM 2017 framework provides a similarly dense narrative description, which was a good prerequisite for the further verification of the RMDM. Another reason for choosing this framework obviously was that the publishing organization COSO thoroughly updated it in June 2017. The second mapping and its results are discussed in Section IV C and D.

B. Main Components

Figure 4 shows the status quo of the advanced ICT risk-meta-data-model (RMDM) after the second mapping. Classes or relationships written in italics are represented in the UML diagram. The RMDM can be divided in five main components. On an abstract level, all classes are derived from class Organisation and further divided in *Input*, *Process*, *Output* and *Actor*. These classes of the first component introduce a fundamental structure to group the other classes within the risk management process. This construction with generalization relationships both introduces an additional inherent structure of the data model and applies generalization and inheritance of attributes by superior classes in order to cope with the rising complexity. A particularity of the class *Actor* has to be underlined. The class *Actor* represents all persons and their responsibilities taken over by organizational entities, persons or roles, e.g., by the risk manager. *Actor* also *owns* a *Process*. However, especially the class *Process* should also be able to summarize all important processes, policies, standards and guidelines that form the operational environment. It is not only an abstract data structure, but rather a hybrid class.

The operative part of the conceptual model and the linked classes can be further divided into three virtual processing parts, which are not explicitly included in the UML diagram in Figure 4 but structurally grouped in line with the virtual workflow collecting input, processing and controlling risks. In the first phase, which summarizes all the different input factors and puts them into a common context, the conceptual model shows the detailed causal chain from the single risk factors to the identified risk, which is in fact a prerequisite for performing an operational risk management process. This architectural characteristic enables a possible ex-post analysis or simulation by means of the provided background information in the input classes to examine their practical influences on the final risk. The resulting risk is only a product of its input factors. The appealed causal chain starts on the left side with a pure *Hazard*, which *threatens* a

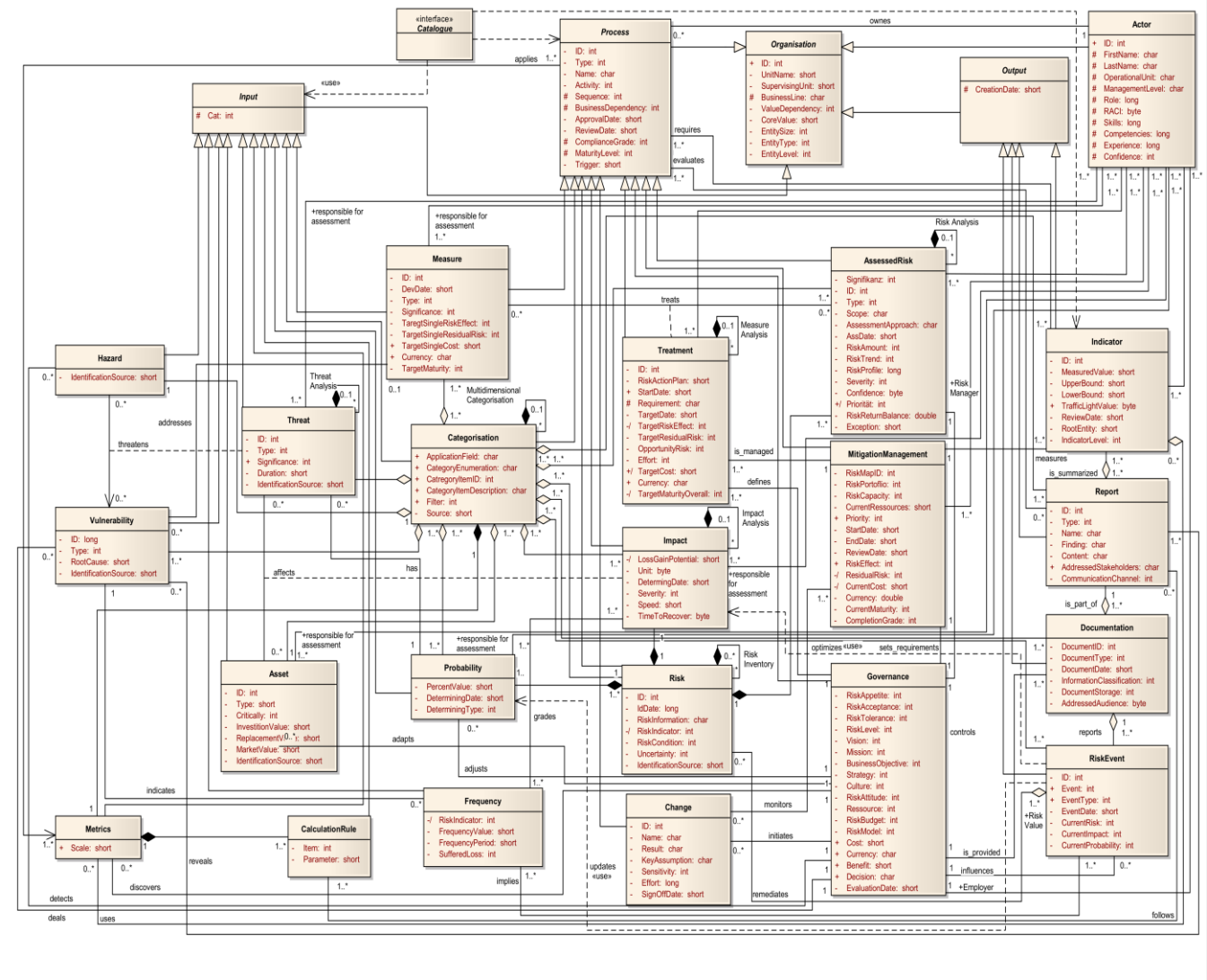

Figure 4. Conceptual ICT risk-meta-data-model (RMDM) described as UML class diagram after the COSO ERM 2017 mapping [own research]

particular *Vulnerability*, resulting in the associated class *Threat*. Hence, the *Threat* explicitly *affects* an *Asset* of the organization, leading to one main risk factor *Impact*, which is also designed as an associated class. The *Threat has* also some *Probability* to materialize, which is the second immediate main risk factor. Typically, the *Risk* can be characterized by its essential components *Impact* and *Probability*, which are often shown in a risk matrix and here designed as composition of both risk factors. However, the *Risk* reflects only the identified risks and does not yet link to a detailed assessment, which the organization is required to do as a next step.

The second phase of the risk management process further processes the risk. It involves the assessment of the previously identified raw risks and linking them with the given influencing factors and framework conditions. Accordingly, the class *Risk* is a composition for *AssessedRisk*. This class records all necessary evaluations of the risks. A *Measure* treats *AssessedRisk*, but there is no indication whether these measures are really applied in this stage. This is indicated by the associated class *Treatment*. In this way, a gradual filter starting from *Risk*, via *Measure* to *Treatment* can be applied. This filter – which could also be interpreted as a second causal chain in the same sense as the risk factors discussed above – allows focusing only on those risks, which should be actively addressed in the risk management process and further reduces the complexity of the model to the high-risk areas according to the individual risk level. Consequently, all selected *Treatments* are managed by *MitigationManagement* during their whole lifecycle. The class *MitigationManagement* represents the fundamental risk portfolio from a manager's point of view. Thus, this class represents the core structure for performing the risk management process within the defined risk management framework over time. After the identification of risks, this stage effectively reduces the amount of relevant risk on which the organization should focus. Finally, management will control the remaining risks by applying a

continuous risk management process. The underlying idea is that the relevant risks which need ongoing attention will be filtered, reduced in their amount and monitored by a cyclic quality process that forces the organization to regularly look at the remaining risks.

The third stage of the operative risk management process represented in the ICT risk-meta-data-model addresses the management's governance and its supporting elements, e.g., key output, risk events, or metrics. The class *Governance* establishes requirements for the class *MitigationManagement* and subsumes all the influencing factors to set up the appropriate risk environment. It holds management information about finance, vision, mission, business objectives, strategy, culture and business context, risk model, attitude, appetite and tolerance etc. It is supported by ongoing *Changes*, which subsume all ancillary activities that support risk management activities, i.e., projects, changes. The class *Categorization* addresses all forms of structuring, e.g., categories, graduations, risk scales, and cluster definitions in the context of risk management efforts, and provides additional structure, while it leaves enough leeway for individual metrics. Consequently, the *Categorization* class has relationships with all the classes that need such a structuring. It is also possible to integrate external catalogues, frameworks, and regulations into the risk management model through the interface class *Catalogue*. The intention of this part is to reflect on the necessary high-level governance of risk management in the responsible organization.

The fifth and final part covers all aspects that are relevant for documentation and measuring performance. This fifth part enables to take a current snapshot of the risk situation and forms a new starting point for a further cycle of the risk management process. Additionally, this part also provides concrete information on actual risk, which helps to achieve a higher maturity degree of the risk management lifecycle. *Documentation* in any form, especially *Reports* or (Key Risk) *Indicators*, has specifying classes, which are implemented as aggregations from the generic structure (*Documentation*) to more quantifiable information (*Indicator*). *Documentation* covers all documents that are relevant for governance decisions and thus creates an information repository. *Metrics* with specified *CalculationRules* stores all kinds of calculation bases, e.g., for Balanced Scorecard, Key Risk Indicators, or Process Performance. This ICT risk-meta-data-model also includes an important feedback loop. The class *RiskEvent* ensures the remediation of risk information based on new findings due to incidents based on real-life incidents. In combination with the class *Frequency*, the quantification of already suffered risk events enables the adjustment of the underlying risk factors, thus increasing the accuracy of further assessments. Finally, intended self-referencing relationships for the classes *Categorization*, *Threat*, *Impact*, *Risk*, *AssessedRisk*, and *Treatment* enable further substantial analysis, e.g., multidimensional assessments of cascading effects if needed. These five main parts of the ICT risk-meta-data-model interlock with one another. Thus, both the continuous elements of the risk management process and the different perspectives of operative process performance and strategic embedding in the organization – in fact the apparent two-tier approach of the discussed risk management frameworks can be reflected in the model.

IV. MAPPING

A. Method for the COBIT for Risk Mapping

The critical success factor for the proper functioning of the meta-modeling idea is the coherent transformation of the information of the selected risk model up to the meta-model while at the same time sufficiently reducing the information content. This transformation is in fact a mapping of all the relevant pieces of information that is necessary for performing risk management with the selected risk model. The risk model COBIT for Risk was selected as the first proof of concept for the metamodeling approach. It provides an appropriate degree of concreteness in order to verify the draft concept that was first introduced in [2].

In a first step, both risk management core processes Evaluate, Direct and Monitor (EDM) 03 "Ensure Risk Optimisation" – the setup of the risk management environment in the organization – and Align, Plan and Organise (APO12) "Manage Risk" – the risk management process as discussed above – were analyzed. All information artefacts mentioned as input or output objects and in the description of the risk specific activities were extracted to a list. These have a different degree of concreteness, which was also assessed. This step was repeated for each of the other twelve supporting processes, which are marked in dark red in Figure 1. This finally resulted in a list of 1619 identified information artefacts, but this list included duplicates, synonyms, and different notations of the same objects, cf. Figure 5. In a second step, all these entries were consolidated in order to even out differences and reduce the amount of information artefacts for further analysis. All entries were transformed into a consolidated object, in fact performing a form of abstraction. This transformation resulted in a list of 26 objects, which corresponds to the column 'synonym' in Figure 5. The purpose of these objects was to set up a data store, leading to a UML class at the end of this process. This abstraction process was conducted as iterative working step because the consolidated object list initiated continuous improvement actions in order to get a coherent list for the subsequent steps. Once the list of consolidated objects had been verified, the consolidated object list was mapped to the classes in the UML diagram. In a third step, the class attributes were revised so that the essential data for risk management fit properly into the appropriate classes.

B. Results of the COBIT for Risk Mapping

The mapping process showed that it is generally possible to transform the essential risk management data from COBIT for Risk up to the meta-level. Small amendments to the draft version of the ICT risk-meta-data-model were necessary after completing the mapping process, e.g., the introduction of the new class *Changes*, which reflects all current change management activities in the considered organization. The

transformation is highly dependent on how concrete the specification of the risk model and its components is. If the risk model leaves too much room for interpretation inconsistencies may appear in the instantiation of the ICT meta-data-risk-model itself. This means that activities without inputs or outputs should be scrutinized. Almost all inputs, outputs and standard COBIT 5 activities specified in the twelve risk supporting processes were unsuitable for the mapping. Thus, certain problems are expected when using ISO 31000 as base risk model because of its highly generic approach. This means that not every risk management framework may be suitable for the mapping due to the different levels of detail of the different frameworks. Furthermore, the framework must provide storage of all kind of documentation that supports the functioning of the management system. Currently, the meta-model includes the dedicated class *Documentation* for this issue. It was originally intended only for risk management documentation, but it has a broader scope, providing a repository for all documentation produced by the applied management system.

Process	Source	Artefact	Level of Detail	Synonym
APO012.01	1	analysis method	medium	Process
APO012.01	1.1	analysis model	low	Process
APO012.01	1.4	assessment of risk attribute	medium	Assessment
APO012.01	2.2	audit	medium	Actor
APO012.01	2.2	business source	low	Catalogue
APO012.01	2.2	CIO office	medium	Actor
APO012.01	1	classification method	medium	Category
APO012.01	1.1	classification model	high	Category
APO012.01	4.1	collected data	medium	Catalogue
APO012.01	1	collection method	medium	Process
APO012.01	1.1	collection model	low	Process
APO012.01	2.3	competition within industry	low	Metrics
APO012.01	2.3	competitor alignment	low	Metrics
APO012.01	2.2	compliance	medium	Requirement
APO012.01	4.1	contributing factor	high	Risk Factor
APO012.01	4.3	contributing factor	high	Risk Factor
APO012.01	3.1	data collection model	low	Process
APO012.01	1.4	data for incentive setting (risk-aware culture)	low	CorporateGovernance
APO012.01	2	data on enterprise`s operating environment	medium	Catalogue

Figure 5. Excerpt of the list of information artefacts of COBIT for Risk [own research]

The first mapping extends the proof of concept that was outlined in [2] to all affected risk management processes of the COBIT for Risk framework. Some small adjustments of the first draft of the ICT risk-meta-data-model were made, but no fundamental changes of the inherent structure of the classes or relationships were necessary. This shows that the ICT risk-meta-data-model is able to represent and store the necessary information for applying the COBIT for Risk framework in principle.

C. Method for the COSO ERM 2017 Mapping

In order to further develop the RMDM in the version of [1], a second mapping with another risk model is performed. The objective of this second round of mapping is to verify the defined class structure and refine the attributes, which were established after the COBIT for Risk mapping. This second mapping aims at ensuring a consistent structure of the RMDM for both underlying frameworks. If this second mapping was also successful, the RMDM could be applied at least for those two risk models, would be more robust, more mature and expected to be applicable in a more flexible way to other frameworks. The assumption is that the adjustments which will be needed to integrate a second risk model should be limited. On the other hand, it is important that the modifications are done carefully because the class structure and especially its attributes must be valid for both risk models.

In contrast to COBIT for Risk, which is in fact a specification of a broad, comprehensive governance framework for risk management, the whole framework COSO ERM 2017 [15] is explicitly designed for risk management purposes. This implies that all five components and the 20 principles – as depicted in Figure 2 – had to be analyzed. According to the applied mapping method, all information artefacts mentioned in these principles have been identified in the narrative description of the framework, finally resulting in 1 935 entries. This list, which is illustrated in Figure 6, has the same structure as the list that was generated for the COBIT for Risk mapping earlier, so that the entries can be easily compared later on. It was remarkable that the information artefacts could be directly mapped to an existing class object that already existed in the RMDM. Consequently, the consolidating intermediate stage for categorizing, harmonizing and finally minimizing of the information artefacts was not needed. Additionally, the first mapping was helpful to leave no room for interpretation. It also ensured a kind of quality control in order to avoid inconsistencies during both mapping processes. Furthermore, it showed that the class structure already has a stable form and is ready for a third risk model integration.

D. Results of the COSO ERM 2017 Mapping

Since the attributes had already been aligned to COBIT for Risk, the necessary adjustments to the attribute's names had to be done very carefully. Therefore, no attributes were deleted and there was no need for this either. The main objective was to provide sufficiently clear mapping paths from an information artefact on the risk model level to a class attribute on the meta-level, regardless of whether COBIT for Risk or COSO ERM 2017 was applied. The second mapping resulted in small adjustments in the names of attributes and even in additional attributes. The detailed changes that were introduced to the RMDM as a result of the COSO mapping were as follows. A self-referenced relationship of the class *Risk* depicts a risk inventory. A direct relationship between *Actor* and *Process* reflects the process ownership. An additional relationship of the *Documentation* and the *Report* class to the *Categorization* class helps to better categorize the different types of documentation and reports. The further attribute 'identification source' defines the origin of the different risk factors. More attributes were added to the classes *Organisation*, *Governance*, *MitigationManagement*, *AssessedRisk* and *Risk*. It can be argued that the reason for these additional attributes is the stronger top down approach of COSO ERM 2017 compared to COBIT for Risk. The additional attributes provide points of references for vision, mission, risk attitude, risk model, culture, risk capacity, risk portfolio, current [assigned] resources, core values, size, type

Process	Source / Section	Information Artefact	degree of cor	Synonym
P8: Evaluates Alternative Strategies	Understanding the Implications from Chosen Strategy	strategy	low	Governance
P8: Evaluates Alternative Strategies	Understanding the Implications from Chosen Strategy	strategy	low	Governance
P8: Evaluates Alternative Strategies	Understanding the Implications from Chosen Strategy	supporting assumptions relative to business context, resources, capabilities	medium	Treatment
P8: Evaluates Alternative Strategies	Understanding the Implications from Chosen Strategy	technical expertise	medium	Actor
P8: Evaluates Alternative Strategies	Understanding the Implications from Chosen Strategy	types of risk	medium	AssessedRisk
P8: Evaluates Alternative Strategies	Understanding the Implications from Chosen Strategy	vision	low	Governance
P8: Evaluates Alternative Strategies	Understanding the Implications from Chosen Strategy	working capital	low	Asset
P9: Formulates Business Objectives	Understanding Tolerance	achievement of business objective	medium	Governance
P9: Formulates Business Objectives	Understanding Tolerance	achievement of strategy	low	Governance
P9: Formulates Business Objectives	Understanding Tolerance	approach for measuring	medium	Process
P9: Formulates Business Objectives	Understanding Tolerance	boundary of acceptable variation	medium	MitigationManagement
P9: Formulates Business Objectives	Understanding Tolerance	business objective	medium	Governance
P9: Formulates Business Objectives	Understanding Tolerance	enhancing value	medium	Asset
P9: Formulates Business Objectives	Understanding Tolerance	management	high	Actor
P9: Formulates Business Objectives	Understanding Tolerance	mission	low	Governance
P9: Formulates Business Objectives	Understanding Tolerance	objective	medium	Governance
P9: Formulates Business Objectives	Understanding Tolerance	outcomes	medium	Governance
P9: Formulates Business Objectives	Understanding Tolerance	performance	medium	Indicator
P9: Formulates Business Objectives	Understanding Tolerance	range of tolerance	high	MitigationManagement
P9: Formulates Business Objectives	Understanding Tolerance	risk	medium	Risk
P9: Formulates Business Objectives	Understanding Tolerance	risk appetite	high	Governance
P9: Formulates Business Objectives	Understanding Tolerance	strategy	low	Governance
P9: Formulates Business Objectives	Understanding Tolerance	tolerance	high	MitigationManagement
P9: Formulates Business Objectives	Understanding Tolerance	vision	low	Governance
P10: Identifies Risk	Using a Risk inventory	category	high	Categories
P10: Identifies Risk	Using a Risk inventory	impact of risks	high	Impact
P10: Identifies Risk	Using a Risk inventory	number of risks identified	high	AssessedRisk
P10: Identifies Risk	Using a Risk inventory	opportunities	medium	Risk
P10: Identifies Risk	Using a Risk inventory	risks	low	Risk

Figure 6. Excerpt of the list of information artefacts of COSO ERM 2017 [own research]

and level of entity. The current status of the RMDM after the second mapping is shown in Figure 4, which can be compared with its previous version in [1, Fig. 3], if needed.

It is remarkable that the concepts of terms and definitions used in the COSO ERM 2017 framework are more consistent than in the COBIT for Risk, resulting in fewer synonyms and discrepancies in terms and notations and making it easy to find double entries. The terms were applied in a highly consistent way throughout the whole framework. Therefore, it was much easier than in the first mapping to perform the consolidation phase. It was almost a straight-forward process to select the right class objects from the RMDM. A key difference compared to COBIT for Risk is that COSO ERM 2017 starts with the risk itself and does not even analyze the previous risk factors before. Consequently, 451 identified information artefacts could be subsumed under the *Governance* class, as many as 66 remained to be subsumed under the class *MitigationManagement* and 223 under the *AssessedRisk* class. In total, this amounts to almost 42 percent of all identified information artefacts of COSO ERM 2017. In contrast, in COBIT for Risk the number of assigned artefacts to these three classes amounts to only 304 information artefacts.

Finally, it shows that all the risk management information that is necessary for applying the COSO ERM 2017 risk model can also be covered by the existing RMDM classes. Due to the fact that the terms and definitions in COSO ERM 2017 are more robust than in COBIT for Risk, some light adjustments of the attribute names make sense and are important. Based on the higher consistency of terms and definitions in the COSO ERM 2017, both the RMDM classes and their attributes pass a kind of consistency check when these adjustments of attributes are performed.

E. Further Research

Further research is still needed to verify the transformation process with two or three other risk management frameworks. This verification should definitely be done for ISO 31000 [3], despite the above-mentioned expectation that the framework will be too generic. The suitability of ISO 31000 should be verified because of its outstanding importance as a world-wide standard. The NIST Special Publications 800-30/-37/-39 [4] [5] [6] also provides the more detailed content that is necessary for the mapping and is thus a good candidate. Moreover, its importance in the US strongly suggest an integration into the RMDM. If it is possible to map their information requirements in the same way as it has been done for COBIT for Risk and COSO ERM 2017, the ICT risk-meta-data-model can be applied at least for these four risk management frameworks, in this way providing an adequately sustainable meta-model solution.

However, the top down approach of the COSO ERM 2017 mapping reveals the inherent problem of adequately reflecting abstract concepts of terms like culture, code of conduct, behavior, expectations or business context, which are not easy to present in the data structure. For the moment, all these aspects have been subsumed under culture and it has not been decided yet how to integrate them into the data structure in more detail.

If the mapping process has been applied several times and the attributes are almost stable (except for a refinement of the definite data types and the visibility properties), the methods can be refined next. The methods of a class should be able to support the complete lifecycle of the concerning attributes. The third area in which refinements are needed is the relationships. It must be verified whether a direct data exchange between the different objects is needed or transitive relationships achieve the same result. Once these

three research questions have been solved, the ICT risk-meta-data-model can be implemented as a first demonstrator, thereby starting the technical verification process. Analyzing these research questions is an ongoing process in order to verify the applicability and utility of the ICT risk-meta-data-model.

In the currently ongoing CERBERUS project of the Austrian National Security Research Program KIRAS [32], the RMDM can serve as a basis for the required overall data model. The objective is that the CERBERUS model holds static data about critical infrastructure objects and combines them with dynamic data obtained from simulations and analyses to represent cross-sectoral cascading risks. The RMDM can serve as a starting point for the development of the CERBERUS data model and can provide structural inputs for risk describing concepts.

The fundamental idea of aggregating risk management data that is stored in different risk models and can be effectively applied when different risk information, e.g., from different companies or organization units that still apply different risk models, need to be migrated. This might be necessary when different companies merge or Comparisons across industry sectors are needed. Another possible application is to use the meta-data-model for training purposes. The model helps to highlight the key elements which are essential for a comprehensive risk management. Moreover, the differences between the risk management frameworks in terms and structure of different risk management models can be illustrated to future risk managers. The implicit comparison between the different approaches gives the training participants an overview of existing risk management approaches that are used in practice.

V. CONCLUSION

This article shows the basic instantiation of two specific risk models – in this case the risk models of COBIT for Risk and COSO ERM 2017 – by means of the conceptual ICT risk-meta-data-model. The objective of the research design is to introduce an ICT risk-meta-data-model for ICT, and to embed it in the context of different established risk models that are commonly applied in the ICT area. The approach of designing a consistent superstructure in form of a meta-model with no need for replacement of the already established ICT risk management models is based on the principle of an ex-post adjustment. Additionally, it provides a data-oriented and more formalized way of overcoming the current organizational and model-related restrictions. The meta-model addresses the whole risk management lifecycle as recommended in [3], from identification, analysis, evaluation to treatment. It reflects both the risk management context and the monitoring and communication requirements for the process. The three main components and the conceptual background of the involved objects are discussed. The findings can be summarized as follows:

- An instantiation of the ICT risk-meta-data-model is generally possible and is a promising possibility to overcome the current situation in ICT, where many different risk models and methods are applied.
- The critical success factor is the coherent transformation of the information of the selected risk model up to the meta-model, while at the same time sufficiently reducing the information content. All essential data of the risk model have an equivalent reference in the superstructure.
- It is crucial to repeat the mapping with other appropriate ICT risk models in order to strengthen the ICT risk-meta-data-model. Moreover, this will reconfirm the general applicability of the meta-data-model and will increase its utility due to having several different risk models mapped to a meta-level.
- The methods and relationships of the objects in the ICT risk-meta-data-model need to be refined before a practical demonstrator can be implemented that can be fed with risk management use cases.

Results show that transferring the general information artefacts specified by COBIT for Risk as well as COSO ERM 2017 into the classes of the meta-model is feasible and promising. The future refinement effort will iteratively improve the ICT risk-meta-data-model in order to further develop and evaluate it and strengthen its applicability for ICT risk management.

ACKNOWLEDGMENT

This work received financial support from the CERBERUS (Cross Sectoral Risk Management for Object Protection of Critical Infrastructures) Project (No. 854766) of the Austrian National Security Research Program KIRAS, Call 2016/2017.

REFERENCES

[1] M. Latzenhofer and G. Quirchmayr, “RMDM – A Conceptual ICT Risk-Meta-Data-Model – Applied to COBIT for Risk as underlying Risk Model,” presented at the SECURWARE 2017: The Eleventh International Conference on Emerging Security Information, Systems and Technologies, Rome, 2017, pp. 117–124 [Online]. Available: www.thinkmind.org

[2] M. Latzenhofer, “Ein Meta-Risiko-Datenmodell für IKT,” in *Bestandsaufnahme, Konzepte, Anwendungen, Perspektiven*, Klagenfurt, pp. 161–173.

[3] International Organization for Standardization (ISO), Ed., *ISO 31000:2009 Risk management - Principles and guidelines*. ISO, Geneva, Switzerland, 2009.

[4] National Institute of Standards and Technology (NIST), U.S. Department of Commerce, Joint Task Force Transformation Initiative Information Security, Ed., “NIST 800-30: Guide for Conducting Risk Assessments.” Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology, Gaithersburg, MD 20899-8930, USA, Sep-2012 [Online]. Available: http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf

[5] National Institute of Standards and Technology (NIST), U.S. Department of Commerce, Joint Task Force Transformation Initiative Information Security, Ed., “NIST 800-37: Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach.” Computer Security Division,

Information Technology Laboratory, National Institute of Standards and Technology, Gaithersburg, MD 20899-8930, USA, Feb-2010 [Online]. Available: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r1.pdf

[6] National Institute of Standards and Technology (NIST), U.S. Department of Commerce, Joint Task Force Transformation Initiative Information Security, Ed., "NIST 800-39: Managing Information Security Risk - Organization, Mission, and Information System View." Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology, Gaithersburg, MD 20899-8930, USA, Mar-2011 [Online]. Available: http://csrc.nist.gov/publications/nistpubs/800-39/SP800-39-final.pdf

[7] Committee of Sponsoring Organizations of the Treadway Commission (COSO) and Price Waterhouse Cooper (PwC), "Enterprise Risk Management - Aligning Risk with Strategy and Performance (Public Exposure Draft)." Jun-2016.

[8] The Stationary Office (TSO), Ed., "Management of Risk: Guidance for Practitioners." 2010.

[9] Information Systems Audit and Control Association (ISACA), Ed., "COBIT 5 for Risk." Information Systems Audit and Control Association, Rolling Meadows, IL 60008 USA, 2013 [Online]. Available: http://www.isaca.org/COBIT/Pages/Risk-product-page.aspx

[10] Information Systems Audit and Control Association (ISACA), "ISACA." [Online]. Available: https://www.isaca.org/Pages/default.aspx. [Accessed: 24-May-2018]

[11] Information Systems Audit and Control Association (ISACA), Ed., "COBIT 5: A Business Framework for the Governance and Management of Enterprise IT." Information Systems Audit and Control Association, Rolling Meadows, IL 60008 USA, 2012 [Online]. Available: http://www.isaca.org/cobit/Pages/CobitFramework.aspx

[12] Committee of Sponsoring Organizations of the Treadway Commission (COSO), *Enterprise Risk Management Framework*. Committee of Sponsoring Organizations of the Treadway Commission, 2004.

[13] Committee of Sponsoring Organizations of the Treadway Commission (COSO), "COSO." [Online]. Available: http://www.coso.org/. [Accessed: 24-May-2018]

[14] Committee of Sponsoring Organizations of the Treadway Commission (COSO), "Internal Control - Integrated Framework." 1992.

[15] Committee of Sponsoring Organizations of the Treadway Commission (COSO) and Price Waterhouse Cooper (PwC), *Enterprise Risk Management - Integrating with Strategy and Performance*, vol. 1. 2017.

[16] D. Karagiannis and H. Kühn, "Metamodelling Platforms," in *E-Commerce and Web Technologies*, vol. 2455, K. Bauknecht, Am. Tjoa, and G. Quirchmayr, Eds. Springer Berlin Heidelberg, 2002, p. 182 [Online]. Available: http://dx.doi.org/10.1007/3-540-45705-4_19

[17] N. Rödder, R. Knapper, and J. Martin, "Risk in modern IT service landscapes: Towards a dynamic model," in *Service-Oriented Computing and Applications (SOCA), 2012 5th IEEE International Conference on*, 2012, pp. 1–4.

[18] Y. Yu, Q. Hao, and P. Hao, "The research and application of enterprises' dynamic risk monitoring and assessment model based on related time series," in *Chinese Automation Congress (CAC), 2017*, 2017, pp. 7407–7410.

[19] T. R. Bezerra, S. Bullock, and A. Moura, "A simulation model for risk management support in IT outsourcing," in *Simulation and Modeling Methodologies, Technologies and Applications (SIMULTECH), 2014 International Conference on*, 2014, pp. 339–351.

[20] D. Wawrzyniak, "Information security risk assessment model for risk management," in *International Conference on Trust, Privacy and Security in Digital Business*, 2006, pp. 21–30.

[21] M. Kakvan, M. A. Mohyeddin, and H. Gharaee, "Risk evaluation of IT service providers using FMEA model in combination with Multi-Criteria Decision-Making Models and ITIL framework," in *Telecommunications (IST), 2014 7th International Symposium on*, 2014, pp. 873–878.

[22] N. C. Pa and B. Anthony, "A model of mitigating risk for IT organisations," in *Software Engineering and Computer Systems (ICSECS), 2015 4th International Conference on*, 2015, pp. 49–54.

[23] M. L. Yeo, E. Rolland, J. R. Ulmer, and R. A. Patterson, "Risk mitigation decisions for IT security," *ACM Trans. Manag. Inf. Syst. TMIS*, vol. 5, no. 1, p. 5, 2014.

[24] C. A. Pinto, A. Tolk, and M. McShane, "Emerging M&S application in risk management," in *Proceedings of the 2011 Emerging M&S Applications in Industry and Academia Symposium*, Boston, Massachusetts, 2011, pp. 92–96.

[25] Q. Zheng and H. Na, "Insurance IT outsourcing risk assessment modeling and empirical study," in *Information and Financial Engineering (ICIFE), 2010 2nd IEEE International Conference on*, 2010, pp. 202–206.

[26] Y. Zhang, B. Hamid, and D. Gouteux, "A metamodel for representing safety lifecycle development process," presented at the 6th International Conference on Software Engineering Advances (ICSEA 2011), 2011, pp. 550–556.

[27] B. Yang and T. Zhang, "A Scalable Meta-Model for Big Data Security Analyses," in *Big Data Security on Cloud (BigDataSecurity), IEEE International Conference on High Performance and Smart Computing (HPSC), and IEEE International Conference on Intelligent Data and Security (IDS), 2016 IEEE 2nd International Conference on*, 2016, pp. 55–60.

[28] F. Cicirelli, G. Fortino, A. Guerrieri, G. Spezzano, and A. Vinci, "A meta-model framework for the design and analysis of smart cyber-physical environments," in *Computer Supported Cooperative Work in Design (CSCWD), 2016 IEEE 20th International Conference on*, 2016, pp. 687–692.

[29] M. Findrik, P. Smith, J. H. Kazmi, M. Faschang, and F. Kupzog, "Towards secure and resilient networked power distribution grids: Process and tool adoption," in *Smart Grid Communications (SmartGridComm), 2016 IEEE International Conference on*, Sydney, Australia, 2016, pp. 435–440.

[30] S. H. Othman and G. Beydoun, "Metamodelling approach to support disaster management knowledge sharing," presented at the 21st Australasian Conference on Information Systems (ACIS), Atlanta, GA, USA, 2010, pp. 1–10 [Online]. Available: http://ro.uow.edu.au/cgi/viewcontent.cgi?article=10789&context=infopapers

[31] S. H. Othman and G. Beydoun, "Model-driven disaster management," *Inf. Manage.*, vol. 50 (2013), no. Elsevier, pp. 218–228, Apr. 2013.

[32] Federal Ministry for Transport, Innovation and Technology (BMVIT) and Austrian Research Promotion Agency (FFG), "KIRAS Security Research: CERBERUS," 2016. [Online]. Available: http://www.kiras.at/en/projects/detail/d/cerberus/. [Accessed: 25-May-2018]