RISKM: A multi-perspective modeling method for IT risk assessment

Accepted for publication at Information Systems Frontiers – Special Issue on Governance, Risk and Compliance-Applications in Information Systems

Stefan Strecker*
University of Duisburg-Essen, Institute for Computer Science and Business Information Systems
Universitaetsstr. 9, 45141 Essen, Germany
Phone: +49 201 183 - 4563
Fax: +49 201 183 - 934563
stefan.strecker@uni-due.de
* Corresponding author

David Heise
University of Duisburg-Essen, Institute for Computer Science and Business Information Systems
Universitaetsstr. 9, 45141 Essen, Germany
Phone: +49 201 183 - 2719
Fax: +49 201 183 - 4011
david.heise@uni-due.de

Ulrich Frank
University of Duisburg-Essen, Institute for Computer Science and Business Information Systems
Universitaetsstr. 9, 45141 Essen, Germany
Phone: +49 201 183 - 4042
Fax: +49 201 183 - 934042
ulrich.frank@uni-due.de

RISKM: A multi-perspective modeling method for IT risk assessment

Stakeholder involvement and participation are widely recognized as being key success factors for IT risk assessment. A particular challenge facing current IT risk assessment methods is to provide accessible abstractions on matters of IT risk that attend to both managerial and technical perspectives of the stakeholders involved. In this paper, we investigate whether a conceptual modeling method can address essential requirements in the IT risk assessment domain, and which structural and procedural features such a method entails. The research follows a design research process in which we describe a research artifact, and evaluate it to assess whether it meets the intended goals. In the paper, we specify requirements and assumptions underlying the method construction, discuss the structural specification of the method and its design rationale, present a prototypical application scenario, and provide an initial method evaluation. The results indicate that multi-perspective modeling methods satisfy requirements specific to the IT risk assessment domain, and that such methods, in fact, provide abstractions on matters of IT risk accessible to both a technical and a managerial audience.

Keywords: IT risk assessment; enterprise modeling; meta modeling; design science research

1. Introduction

Information technology (IT) related risks pervade organizations from IT operations to corporate strategy (Westerman and Hunter 2007). In the past, assessment of IT-related risks has focused on determining tangible IT assets, internal and external threats to those assets, and the vulnerability of assets to threats (Rainer et al. 1991). Risk assessment has been viewed primarily as a technical, security-related exercise with only marginal consideration given to strategy and business performance (Loch et al. 1992). Its role changed when IT-related risks were revealed to have been major factors in significant business losses. For example, a large French bank lost several billion Euro when weak systems authentication allowed a trader to conduct unauthorized transactions (Sayer and Wailgum 2008). As a consequence, IT risk assessment has received considerable attention from senior management (Rogers et al. 2008) and developed into a key managerial task in the context of IT governance (Weill and Ross 2004). As part of its reinterpretation, IT risk assessment has seen its scope widening to the organizational context into which information technology is embedded (Salmela 2008), i.e., the organizational action system, its institutions and actors, their roles and activities as well as to intangible assets such as know-how of personnel and information resources (Gerber and Solms 2005). Increasingly, IT-related risks are reflected in the light of corresponding business opportunities arising from the use of IT (Westerman and Hunter 2007). IT risk assessment has also received attention due to recent legislation, e.g., the Sarbanes-Oxley Act of 2002 and the Directives 2006/43/EC and 2008/30/EC of the European Parliament and of the European Council. Both regulations mandate documentation of IT-related risks to make threats to the organization traceable and transparent. Moreover, organizations are required to document risk factors, locations of risk exposure as well as the measures and processes in place to counter risk exposure (Carnaghan 2006).

Organizations responding to these changing environmental conditions face a number of challenges: Multiple, often hidden interdependencies exist between risk factors, IT assets, and the surrounding action system (Willcocks and Margetts 1994). IT-related risks and opportunities occur at several organizational levels beyond IT operations and IT projects (Bandyopadhyay et al. 1999). Consequently, stakeholders with different professional backgrounds and perspectives on matters of IT risk are involved (Gemmer 1997), so stakeholders may be drawn from the ranks of IT and project management, line and top management, or internal and external auditing. Stakeholder involvement and participation are key success factors for IT risk assessment (Hatfield 2002; Heemstra and Kusters 1996). Involvement and participation presupposes a shared understanding of IT risk matters, which in turn implies a common conceptual framework of terms and their semantics. As IT risk assessment is often conducted in teams (Gemmer 1997) involving group communication and team decision making on IT risk matters (Klinke and Renn 2002), effective and efficient communication among these stakeholders depends on conceptualizations adequate to the stakeholders' differing perspectives (McGaughey Jr. et al. 1994), their perceptions of and attitudes towards risk (March and Shapira 1987). IT risk assessment constitutes a group process involving complex tasks such as identifying and analyzing risk factors or decision-making, e.g., on appropriate countermeasures, on diverse organizational levels.

These observations motivate research on conceptual modeling methods for IT risk assessment (e.g., zur Muehlen and Rosemann 2005; Sienou et al. 2008). Modeling methods in general and those based on a domain-specific modeling language (DSML) in particular promise to support an IT risk assessment processes effectively, e.g., by providing dedicated concepts for analyses and decision-making and by providing a conceptual foundation for developing dedicated IT risk management systems. Organizational use of conceptual modeling for documentation and communication (Davies et al. 2006) as well as essential working hypotheses—for instance that visual representations of the subject matter reduce complexity (Wand et al. 1995; Frank 1999; Wand and Weber 2002)—suggest that dedicated conceptual modeling methods for IT risk assessment are of practical relevance to organizations.

The present work follows a design research process to develop a multi-perspective modeling method for IT risk assessment and to investigate how its structural and procedural features can satisfy essential requirements in the IT risk assessment domain. The method, RiskM, consists of a domain-specific modeling language, RiskML, its graphical notation and a corresponding process model, RiskPM, to prescribe their use for IT risk identification, analysis, and prioritization. The method's main purpose is to support IT risk assessment group processes by reducing the complexity inherent in IT risk assessment and by providing abstractions tailored to the perspectives of stakeholders. Thus, RiskM is aimed at fostering and facilitating communication and collaboration among stakeholders involved in IT risk assessment. It also aims to increase transparency of IT risk matters, specifically by visually flagging locations of risk exposure, and by improving traceability of risk factors and the countermeasures in place to treat risk exposure.

The next section discusses the epistemological conception underpinning the research on RiskM. Requirements and key concepts of the IT risk assessment domain are reconstructed in Section 3. Section 4 reviews related work and identifies areas for potential improvements over existing conceptual modeling approaches to IT risk assessment. The design rationale of the structural specification of the method, its meta model, is discussed in Section 5 along with a prototypical application scenario illustrating the corresponding process model. An initial method evaluation is provided in Section 6. The paper concludes with a discussion of findings and limitations in Section 7.

2. Research Method

The artifact investigated in this research is a modeling method; a linguistic artifact consisting of a conceptual modeling language —a modeling grammar (Wand and Weber 2002)— and a process model to guide the use of language constructs. The main challenge for conceptualizing research that is aimed at the development of modeling methods as artifact is their justification according to scientific standards (Frank 2006; Schelp and Winter 2006). The success of using a modeling method depends on various factors—qualification, previous experience with other methods, time to learn the method, and attitude towards new methods—that not only vary between different groups but also within a group in time. Furthermore, with respect to the targeted domain, we assume that prospective method users do not have a clear understanding of current and future applications of conceptual model-based IT risk assessment methods and are, hence, not *yet* able to evaluate their practical utility. Hence, field studies to test a newly conceived modeling method are not satisfactory due to subject contingency.

As a result of these considerations, our work is grounded in an approach to guide the configuration of research methods (Frank 2006). The approach suggests two main guidelines for the research process: transparency (of assumptions) and multi-criteria justification. Transparency means that all non-trivial assumptions about the method design are identified throughout the research process. This pertains to requirements, design decisions, and the evaluation of the artifact against the requirements. To guide the method's development, its purpose and design goals need to be substantiated by requirements. If a requirement is not obvious or deducted from established knowledge, it is based on an assumption. The construction of the method or parts of it, in this case of a domain-specific modeling language, implies choices of design alternatives. Again, the assumptions underlying non-trivial design decisions are to be made explicit. Finally, the resulting method is evaluated by comparing its features against the design goals and requirements. In some cases, checking if a requirement is met will be straightforward. A requirement may be as simple as the presence of a certain feature, for example. In other cases, however, evaluation requires assumptions; as is particularly the case with respect to requirements that relate to user acceptance or perceived benefit. Multi-criteria justification is based on the belief that there are various approaches available to substantiate an assumption. The selection depends on the theory of truth that is regarded as suitable, and the feasibility of corresponding justification procedures. Justification procedures include empirical tests (correspondence theory), discursive evaluation (consensus theory) and coherence with an existing body of accepted knowledge (coherence theory). The configuration approach provides criteria to guide the selection of justification procedures (Frank 2006, p. 48). Combining the selected justification procedures results in the configuration of a research method that accounts for the epistemological particularity of the corresponding research. Note that the most appropriate justification procedure may not be practicable, perhaps because of the lack of time or resources or some other obstacle. In this case, the configuration approach recommends applying the second or third best option. Applying such a configuration approach does not guarantee a convincing justification. It does, however, contribute to an incremental justification and supports the further evaluation of the artifact by making it clear where its justification is still not satisfactory.

The justification procedures used in the present research are a combination of discursive evaluation and the application of the coherence theory of truth, i.e., substantiating assumptions by reference to a body of literature. Empirical tests are not included due to subject contingency and lack of feasibility at present. Note that this does not mean that empirical tests are not suitable for testing modeling methods in general. If model-based IT risk assessment methods are more widely used, it can be more promising to pursue an empirical evaluation. Discursive justification in its ideal form would involve a rational discourse within a group of outstanding experts. A consensus on the truth value of a proposition would then be regarded as a satisfactory—albeit preliminary—test. This study applied a relaxed form of discursive evaluation. It starts by establishing with high-level assumptions on design goals, which are likely to be agreed upon by many with knowledge of the domain of IT risk assessment. It proceeds to analytically deduce more specific requirements, which can be assumed to elicit consensus, and which are substantiated by the existing body of literature. In some cases, this approach will produce only weak justifications—a result which may be explained by the idiosyncrasy of the topic. Note that in order not to impair the paper's readability, not every assumption will be explicitly marked as such. In terms of Verschuren and Hartog's (2005) idealized design research process, this paper focuses on requirements and assumptions (phase 2; corresponds with section 3), structural specification (phase 3; corresponds with section 5), prototype (phase 4; corresponds with section 5.3), and evaluation (phase 6; corresponds with section 6).

3. Requirements and key concepts

This section refines the high-level requirements mentioned in the introductory section—reducing complexity, fostering communication and collaboration, improving transparency of IT risk matters—to establish six domain-specific requirements that a method aimed at supporting IT risk assessment should satisfy. It also summarizes the initial conceptual reconstruction of the technical terminology used in the IT risk assessment domain by identifying essential domain-specific concepts (cf. Figure 1). The requirements and key concepts guide the development of the RISKM method. They also structure the analysis of related work in the next section and serve as a framework for method evaluation in Section 6.

IT risk assessment as a group process involves stakeholders with different professional backgrounds and responsibilities as well as specific sentiments about risks and their effects (Clemen 1999; Hatfield 2002). Rainer et al. (1991, p. 144) underline the importance of management participation along the entire length of the risk management process. Therefore, IT risk assessment methods need to take the perspectives of stakeholders with different professional backgrounds – from IT operations to management – into account.

> *Requirement 1 – Multiple Perspectives: A method should provide perspectives specific to (groups of) stakeholders involved in the group process. A perspective should, as far as possible, correspond with the abstractions, concepts and (visual) representations known and meaningful to the targeted (group of) stakeholders. All perspectives should, on the other hand, be integrated with each other to foster cross-perspective communication and cooperation.*

Risk as the core concept of the domain has been described as an elusive term prone to misinterpretation (Ward and Chapman 2003) that has led to contradictory terminological conceptualizations (Crouhy et al. 2001; Mun 2004). Ward and Chapman (2003) claim "an emphasis, if not a pre-occupation, with threats rather than opportunities" in the everyday business use of the term "risk"—despite other conceptions which define risk as including both upside *and* downside risk. Its controversial connotations suggest introducing a counterpart to avoid terminological confusion and to clearly delineate upside from downside risk; moving from the suggestion by Ward and Chapman, an obvious choice is to accompany the term "risk" with a counterpart termed "chance". In the spirit of Willcocks and Margetts (1994), a broad risk and chance definition is employed: a risk is defined as a subjectively perceived threat to achieving organizational goals, while a chance is defined as a subjectively perceived opportunity to achieve organizational goals. Risks and chances are considered as uncertainties, in that their probability of occurrence as well as their impact is uncertain and, can at best be assigned estimated values. These uncertainties are linked to organizational goals and work on one or more tangible (e.g., hardware) or intangible (e.g. an information asset or business process) reference objects for which organizational goals are defined.

Requirement 2 – Organizational Context: A method should account for both IT-related risks and chances and link them to the surrounding action system composed of all relevant organizational entities such as corporate goals, organizational units, and business processes.

The pervasive use of IT in organizations entails interdependencies among the reference objects, as between a hardware device and the software running on it or between employees and their access to an information system. A method for IT risk assessment is thus required to identify and evaluate IT-related risks not only at the IT operations level but also to account for cause-and-effect relationships at all other relevant organizational levels—from IT services to business processes to value chains up to the inter-organizational level (Bandyopadhyay et al. 1999).

Requirement 3 – Multiple Organizational Levels: A method should account for cause-and-effect relationships of IT risks and chances at multiple organizational levels, from IT operations to business processes to effects on value chains and the organization as a whole.

Klinke and Renn (2002) assert that identification and evaluation of risks and their cause-and-effect relations are often affected by subjective perceptions, personal experience, and divergent assumptions of the participants in the risk management process. Heemstra and Kusters (1996) point out that risk evaluation should also consider qualitative measures like textual descriptions, to assess risks and chances besides risk quantification in order to account for the difficulties in quantifying and estimating respective (monetary) values (cf. also Gerber and Solms 2005).

Requirement 4 – Quantitative Values and Qualitative Descriptions: A method should provide means for risk quantification where possible and means for qualitative risk description where quantification is either not feasible or not economically justifiable.

The IT risk assessment process is subject to external auditing by virtue of national and international regulations. Legal regulations mandate establishing, managing and documenting risk exposure, internal controls and subsequent audit risk assessment as means to ensure compliance with its norms (Carnaghan 2006), e.g., Section 404 of the Sarbanes Oxley Act of 2002.

> *Requirement 5 – Compliance: A method should support compliance validation and auditing procedures, e.g., by representing the concepts built into regulations, standards and frameworks such as COBIT, or by (possibly partially automated) validation of internal controls.*

Several phase models have been proposed to structure the IT risk assessment process. Risk assessment precedes risk management and includes risk identification, risk evaluation/analysis and risk prioritization (Heemstra and Kusters 1996). The actual risk management process involves risk treatment through risk-reducing measures as well as risk monitoring and reporting (Bandyopadhyay et al. 1999). It is recommended to implement it as a continuous, iterative process (Rainer et al. 1991). Hence, the IT risk assessment process involves frequent transitions between IT risk identification, analysis, and prioritization.

> *Requirement 6 – Multiple Phases: A method should account for the multiple phases of the IT risk assessment process and facilitate transitions between phases, as from IT risk identification to risk analysis.*

Developing a domain-specific modeling language requires reconstructing the key concepts of the targeted domain. Reconstruction of domain-specific concepts is an iterative process involving more than the identification of candidate classes, their attributes and relations. Instead it requires, for instance, the identification and resolution of terminological ambiguity and truncation, which may in turn require the introduction of additional abstractions. That in turn may require the shaping of their semantics. This implies interpretation of observed terms and concepts and of design abstractions appropriate for further purposes, analyses and applications.

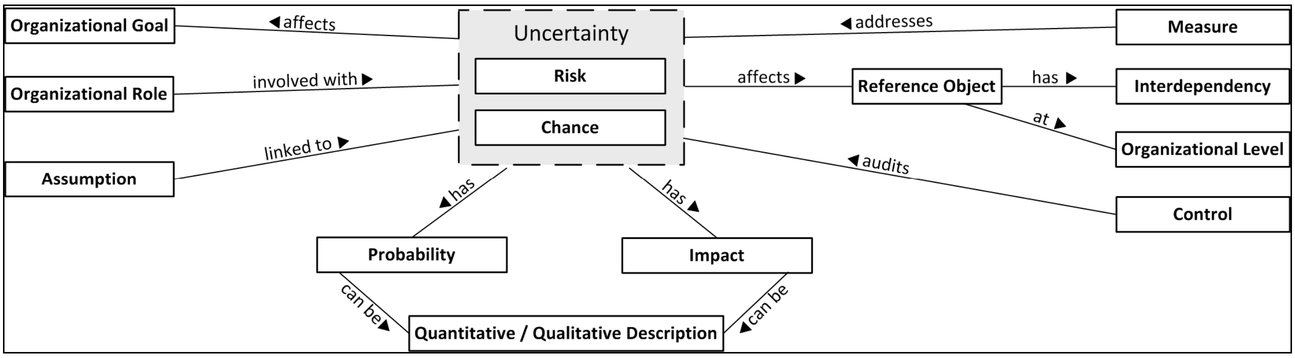

Figure 1 – Semantic net of key domain concepts as preliminary step towards method design.

4. Related work

Apart from Scheer's early work on the event-driven process chain (EPC) (Scheer 1992, 1999), zur Muehlen and Rosemann (2005) are among the first to consider supporting IT risk management through domain-specific conceptual modeling. Their approach extends the EPC approach with concepts for goals and reference objects (applications, data, and human resources). It further builds upon a differentiated conceptual model of risk types (e.g., structural, technological, and organizational). Based on these building blocks, the authors propose four diagram types for modeling risks: a risk structure diagram that represents the aggregation/specialization relationships of risks; a risk state diagram for modeling the cause-and-effect relationships; an EPC notation where risks are associated with activities; and a risk goal diagram that illustrates relations between risks and the business processes' goals. Hence, it is an approach primarily aimed at identifying and annotating risks associated with activities in business processes, and at the semantically-rich documentation of those risks, in terms of their relationship to business goals. Although reference objects other than process activities are mentioned, the proposed modeling approach does not explicitly account for risks associated with IT assets, for example. They do not discuss modeling concepts for chances corresponding to risks, or assumptions associated with risks.

The contribution by zur Muehlen and Rosemann (2005) sparked further work on representing risk in conceptual models. Sienou et al. (2007) specify a graphical risk modeling language that is defined by an elaborate meta model comprising more than 20 meta types. Since attributes are missing from the meta model, the semantics of its concepts are partly up to interpretation. The concept risk at the heart of the meta model is further specified (in terms of associations to other meta types) by an identity, a state, one or more categories as well as by several contextual aspects, like time and space. The meta model provides concepts to represent causes of risks, to specify the context in which to interpret risks, and concepts to capture means to deal with risks. A graphical notation redefining the EPC notation is developed that, among other functions, specifies several relationship types firstly among risks (aggregation and specialization), secondly between risk and events (called "causality relation"), thirdly between risks and assets ("impact relation"), and finally between risks and categories ("classification relation") (Sienou et al. 2008, p. 25). The risk modeling language is integrated with a business process modeling language through common concepts at the meta level (Sienou et al. 2008, p. 24). Instances of the meta type 'risk' can be associated with instances of the meta types 'business process' and 'enterprise activity'. Later, the authors show a risk scenario in an extended EPC diagram (Sienou et al. 2008, p. 27). The meta model integration aims at mapping terms from the risk management domain, like assets and risk factor, to the business process management domain (Sienou et al. 2008, p. 23). The authors admit that not all terms can be mapped and suggest keeping the semantic differences in place instead of introducing further abstractions.

Sadiq et al. (2007) address the related problem of enriching business process models with models of internal controls to facilitate compliance validation. In contrast to the integrative approaches discussed above, they separate business process modeling and the modeling of controls for pragmatic reasons: "prematurely load[ing] business process models with compliance controls will be highly problematic from a practical standpoint" (Sadiq et al. 2007, p. 151).

Table 1: Synopsis of key domain-specific concepts in related work

Key concept	(zur Muehlen and Rosemann 2005)	(Sienou et al. 2007; Sienou et al. 2008)	(Lu et al. 2008; Sadiq et al. 2007)
Risk / Chance / Uncertainty	Wholly negative conception; includes impact and probability	'Risk' subsumes both negative (risks) and positive (chances) aspects; includes impact and probability	Implicitly modeled as part of internal control; no impact or probability
Goal	Indirectly: Goals of Business Processes	Mentioned as one instance of 'Asset', but not specified further	—
Reference Objects	'Process activity'	'Process activity'	'Process activity'
Assumptions	—	—	—
Quantification/ Qualification	Monetary quantification mentioned, but not specified in meta model	Monetary quantification mentioned, but not specified in meta model	—
Measure	Realized by 'Mitigation'	Realized by 'Activity'	Realized by alternative control flow (i.e., process activities)
Relationships	Generalization, Aggregation, and Cause-Consequence-Relationship	Generalization, Aggregation, Risk-To-Risk-Relationship	—
Organizational Role	—	'Stakeholder'	—
Control	—	'Risk Control', but not further specified	Control specification based on modal logic
Metric	—	'Risk Indicator', but not specified further	—

Instead, the authors propose to keep models of internal controls separate from associated process models. Their approach starts from textual descriptions of controls in terms of normative statements such as "The creation and approval of purchase orders must be undertaken by two separate purchase officers" (segregation of duty) as mandated, for example by the Sarbanes-Oxley Act of 2002. The textual descriptions of internal controls are translated into a formal representation based on a modal logic which can be used to reason about compliance violation (Lu et al. 2008). A procedure to link the logic-based statements about internal controls to process models is described, so that clauses appear as process annotations. The authors propose using these enriched process models as a starting point for a "compliance by design" (Sadiq et al. 2007, p. 161) approach, which performs compliance validation at process the time of design, while maintaining process models and models of controls independently. Table 1 highlights key domain-specific concepts in earlier works on conceptual risk modeling and summarizes their conceptualizations.

5. Method Specification

5.1 Conceptual foundation

The RISKM method is based on the Multi-Perspective Enterprise Modeling (MEMO) method (Frank 1994; 2002). The rationale for choosing MEMO over ARIS (Scheer 1992, 2000) or ArchiMate (Lankhorst 2005) or similar methods, is based on several considerations: (1) MEMO provides an extensive set of constructs for modeling IT assets, organizational goals, organizational roles, and organizational units that are relevant to IT risk assessment; (2) in contrast to commercial approaches, like ARIS, the specifications of the MEMO method—especially its meta models—are freely available and documented in several publications; and (3) MEMO is based on a language architecture extendable through domain-specific modeling languages (Frank 2008). In MEMO, domain-specific modeling languages are specified using the MEMO Meta Modeling Language (MEMO MML; M_3 level in Figure 2). The use of the same meta modeling language for defining and reusing common concepts at meta level (M_2) leads to integrated models at type level (M_1), as in a business process model integrated with a model of an IT assets integrated with a model of IT risks and chances.

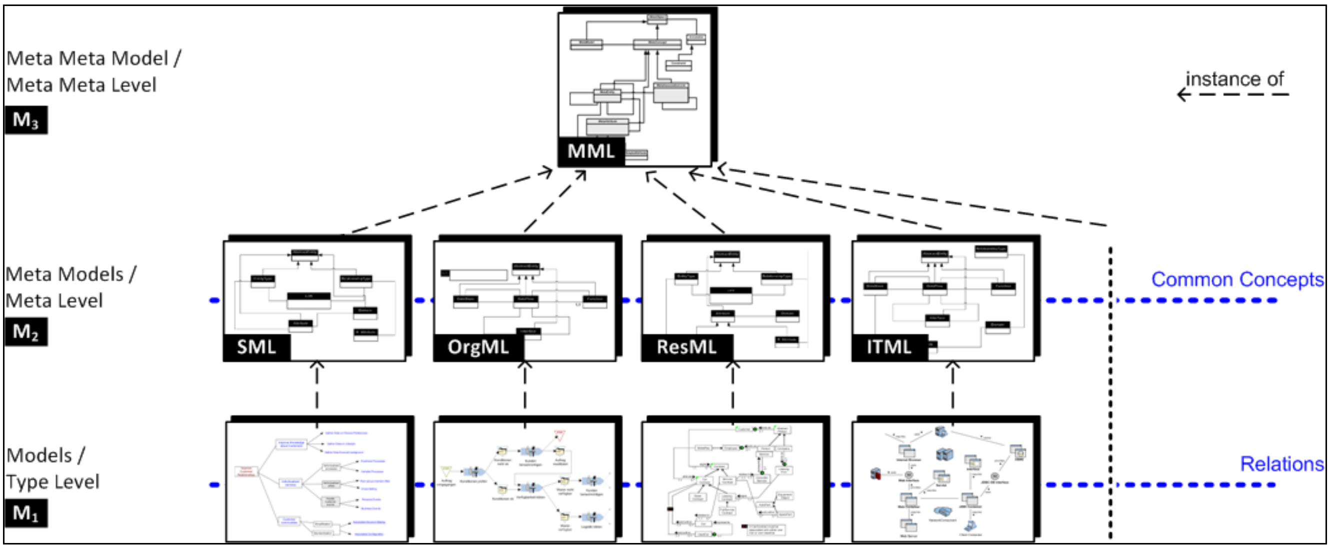

Figure 2 – MEMO language architecture

Using MEMO as a conceptual foundation for RISKM allows the reuse of modeling concepts from existing modeling languages for risk modeling. Of particular importance for risk modeling are, for instance, concepts for modeling business processes (to determine the impact of an IT-related uncertainty on the organization), goals and strategies (to analyze risks in terms of their deviation from business objectives), and IT assets. Each modeling language in MEMO provides specific concepts and abstractions for the aspects they focus on. For example, the strategy modeling language (MEMO SML) includes concepts like 'strategy' and 'goal' and offers diagram types like 'strategy nets' and 'value chains'; the organization modeling language (MEMO ORGML) provides concepts for modeling business processes and organizational structures like 'process', 'event', and 'organizational unit' (Frank 2002); and the resource and the IT modeling languages (MEMO RESML and MEMO ITML) allow modeling of organizational resources in general (e.g., 'human resource'), IT assets in particular (e.g., 'hardware', 'software', 'ERP system'), their relationships to each other (such as 'uses' or 'comprises') and to the business processes they are used in (Frank et al. 2009). Figure 3 shows key notational elements and principal levels of analysis supported by the MEMO family of modeling languages. It includes an IT resource model at the level of IT operations, a business process model showing an aggregated process ("Picking Process") and its disaggregated control flow, as well as a value chain model and an associated business objective ("Goal").

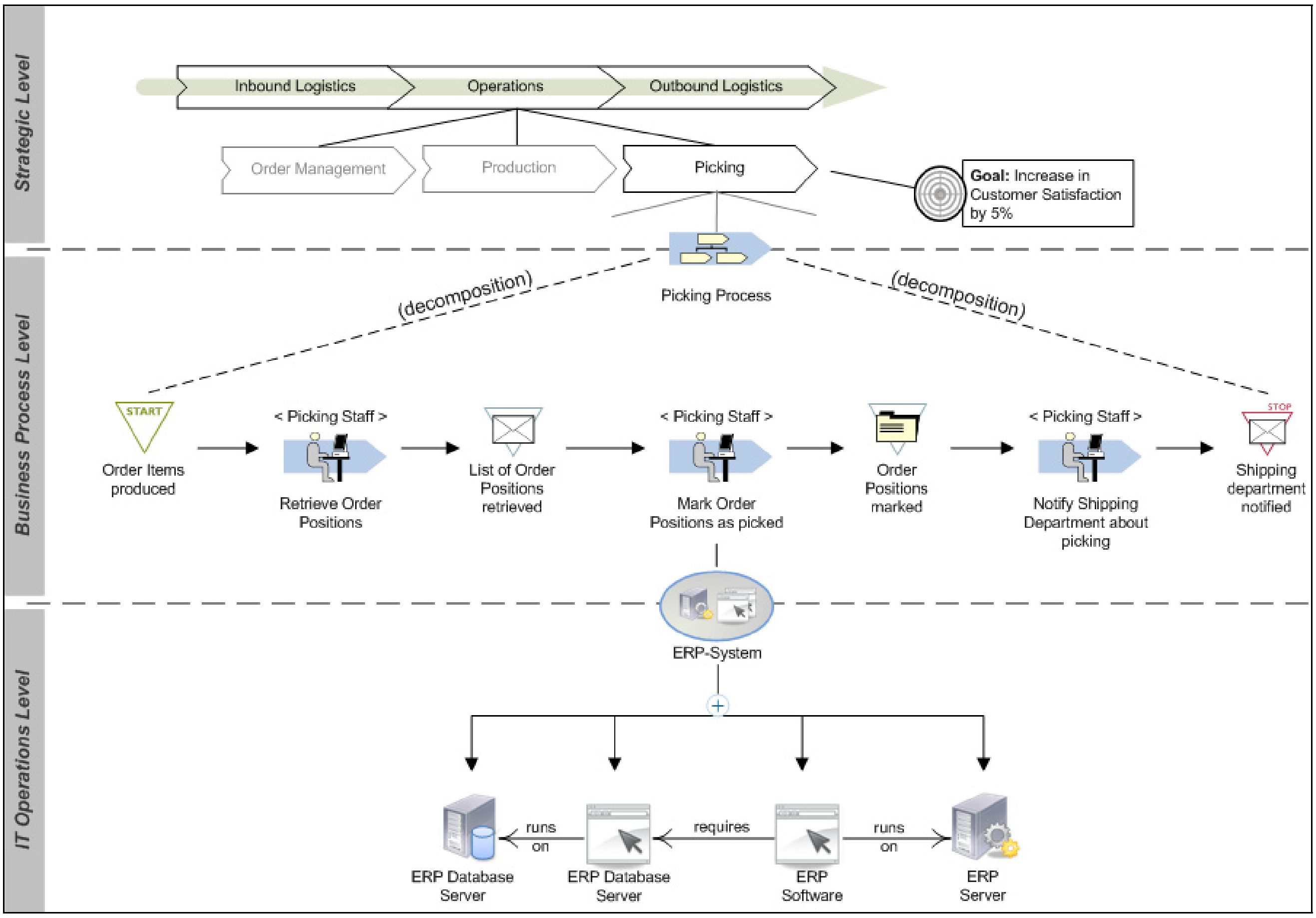

Figure 3 – Key notational elements and principle levels of analysis in MEMO

5.2 Specification of the MEMO RISK Modeling Language

RISKML is specified as a meta model in the MEMO MML (an excerpt of the meta model showing key concepts is depicted in Figure 4). In the following, we introduce the key concepts of the modeling language and discuss selected design decisions with regard to the requirements discussed in Section 3 and to the related work reviewed in Section 4.

A first design decision pertains to the very conception of uncertainties. With respect to *Requirement 2*, RISKML applies a notion of uncertainties that extends the conception suggested by Sienou et al. (2008): an uncertainty represents a probability of occurrence of an event that—if it occurs—will either positively influence (create a chance) or negatively influence (create a risk) the achievement of organizational goals (*influences Goal*; cf. Figure 4). Since these two concepts share essential features while at the same time differing in specific attributes, we propose a meta type *Uncertainty* that is a generalization over the meta types *Risk* and *Chance*. Contrasting with the work by Sienou et al. proposing a single meta type (cf. Section 4), this conceptualization allows the modeler to clearly distinguish between positive and negative aspects—risks and chances—and enables dedicated analyses of dependencies between risks and chances, for example, to denote risks and chances that have to be considered in conjunction with each other (*ChanceRiskRelationship*).

Furthermore, in an extension of the related work, the key concepts of RISKML are enriched with further semantics by providing additional attributes. The main attributes of *Uncertainty* are *courseOfEffect*, to describe the estimated devolution of the effects over time (e.g., instantaneously and in total, or longer-term and dispersed) and thus support detailed planning of (in this case presumably reactive) measures, and *uncertaintyEffect*, which pertains to the effects associated with an uncertainty. In this context, the main challenge is to provide a specification that supports the user in applying different levels of formalization for modeling these effects (cf. *Requirement 4*). The attribute type *EffectSpecification* is introduced to provide such a flexible specification (cf. Figure 5); it allows the modeler to specify statistical distributions for uncertainties supporting quantitative risk assessment techniques, or to describe uncertainties informally through textual description or by using ordinal scales such as the common “high”, “medium”, or “low” differentiation (Heemstra and Kusters 1996; Kliem 2000).

An uncertainty can further be characterized by its *visibility* (how observable are the effects of an uncertainty in case of its occurrence?) and a *dataQuality* (how reliable are the data the effect specification is based on—especially in case of a statistical specification?). Additionally, we suggest annotating *assumptions* (what are the underlying assumptions about the uncertainty and how are they justified?), and an *originator* (who is the originator of the modeled uncertainty, its assumptions, and its justification?). Specific attributes of *Risk* are *durability*, which contains information about the risk's frequency of change perhaps due to changes of the reference object such as system reconfiguration or software updates; *exigence*, which allows for the marking of those risks that deserve special attention due to factors like regulatory conditions; and a statement about the reversibility of the effects of a risk (*isReversible*). To support enterprise-specific adaptations of the language, it is also possible to define customized attributes by instantiating the meta type *UncertaintyAttribute* (not shown in the meta model excerpt). With respect to tool support (e.g. a meta modeling environment such as the Eclipse Graphical Modeling Framework), such customizations based on instantiation promise to be more easily comprehensible and applicable for modelers and to require less software and model maintenance efforts than customizations based on modifications of the meta model.

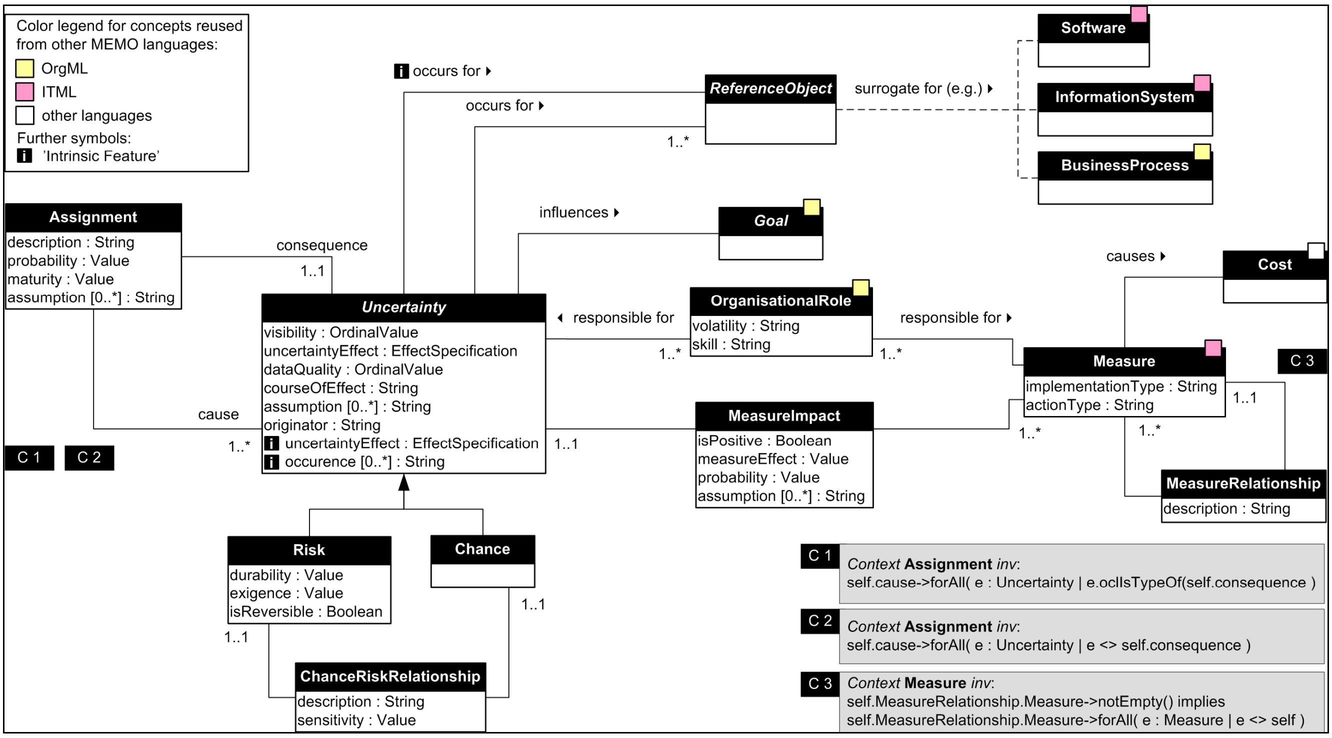

Figure 4 – Excerpt of the RiskML meta model (cardinality 0..* omitted for reasons of clarity)

A further design decision pertains to the organizational context, since IT-related risks and chances may affect various kinds of reference objects at different organizational levels (cf. *Requirement 3*). In the meta model, this is indicated through the abstraction *ReferenceObject*, which serves as a surrogate for relevant meta types. Due to the integration of RiskML with the enterprise modeling approach MEMO (cf. Figure 2), meta types deemed as relevant reference objects for uncertainties can be reused from other MEMO languages (indicated by the white rectangle in the concepts' header in Figure 4); this includes not only a meta type for process activities (*BusinessProcess*) as in related work, but also meta types for, e.g., IT-related reference objects such as *Software* or *InformationSystem*. This explicit association of uncertainties to originating reference objects facilitates the analysis of uncertainties ascribed to specific reference objects. Assuming that relationships among reference objects have already been modeled in business process and resource models, it, moreover, allows for identification of uncertainties of composite reference objects that are ascribed to their constituent elements, e.g., *Software*, *Hardware*, and *IT personnel* in charge of system maintenance with respect to the composite reference object *InformationSystem*. This also permits the reduction of the amount of modeling concepts without losing semantics: In contrast to the ARIS approach (zur Muehlen and Rosemann 2005, p. 69), RISKML does not comprise a differentiated risk typology at meta level. Rather, it subsumes different kinds of risks in a single meta type, while providing the semantics of risk typology at type level by associating different types of reference objects, such as IT assets ('technological risks') or business processes ('structural risks'). This design rationale is based on the hypothesis that fewer modeling concepts reduce the burden on the modeler and reduce learning efforts, which promises to foster acceptance and applicability of the language.

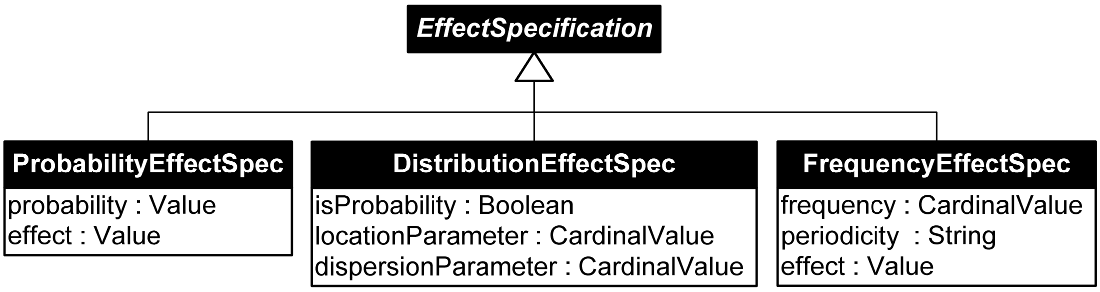

Figure 5 – Meta attribute type for the specification of effects

A third design decision refers to the differentiation of type and instance. In contrast to Sienou et al. (2007), we deliberately distinguish between type and instance level. As Figure 2 indicates, the application of the RISKML results in models at type level (M_1) and describes particular types, (e.g., business process types, resource types etc) found in an enterprise; an instantiation of, for example, the meta type *Risk* is a risk type, i.e., an abstraction over all corresponding instances in the real-world. Hence, the value of *uncertaintyEffect* generalizes over all instances of this uncertainty, which implies that it represents an average of the respective instances. The focus on types rather than instances reduces the complexity of the domain by focusing on those concepts that are pivotal for certain types of analyses and by abstracting from irrelevant technical detail. While this is satisfactory in many cases—especially in an *a priori* risk assessment when reliable data is rarely available—and promotes collaboration and communication between stakeholders, it can be useful and sometimes is even necessary to denote specific information at the instance level (M_0; omitted in Figure 2), as when an effect specification applies to an instance (or a set of instances) of a reference object.

This type-instance issue occurs in particular when developing domain-specific modeling languages (cf. e.g., Kirchner 2005, p. 177), and has long received attention in conceptual modeling research (cf., e.g., Atkinson and Kuehne 2008; Odell 1998). For reasons discussed in detail in Frank (2008), we employ the meta modeling concept of "intrinsic feature". An intrinsic feature is an attribute or an association that reflects a characteristic that—in the language specification—is associated with types but applies only at the instance level. Hence, an intrinsic feature within a meta model is *not* instantiated at the type level, but at the instance level only. In the meta model of RISKML, the intrinsic association *occurs for* allows the assignment of sets of instances of a reference object type to an instance of *Uncertainty*. Thus, it is possible to model specific risks—including statistical distributions for a probability—that apply to specific resource instances, like a batch of hard disks with specific failure probabilities provided by the manufacturer. An example of use of an intrinsic attribute is *occurrence*: This attribute serves to document actual occurrences of uncertainties with timestamps of when the event occurred, for example, which then allows information such as 'Risk State' to be represented as proposed by Sienou et al. (2007). By documenting such information, *ex post* analyses based on historical data are supported.

Finally, IT risks and IT chances, respectively, are often interrelated in terms of cause-and-effect relations (cf. *Requirement 3*): An IT risk can be the cause of another IT risk; in the same way, an IT chance may lead to another IT chance. Such relationships are represented by *Assignment* (cf. Figure 4), which enables the allocation of root cause uncertainties (role *cause*) to affected uncertainties (role *consequence*). Causes can either be assigned individually or as composites (corresponding to the logical connectors ‘AND’ and ‘OR’): AND-assignments are modeled by using several links from the causes into the same instance of *Assignment,* and express the situation where only the conjoint occurrence of causes evokes the consequence. OR-assignments are modeled using separate instances of *Assignment* and denote independent cause-and-effect relations. A prominent example for a composite IT risk associated to an information system is the IT risk “system breakdown” that occurs if either of the two IT risks “breakdown of regular power supply” and “breakdown of uninterrupted power supply unit” occur (AND-semantics), or, for instance, the risk “hard disk failure” occurs (OR-semantics) (cf. Figures 7 and 8). Such defined types of cause-and-effect relations allow the tracing of uncertainties and their effect relations along different organizational levels, such as from IT assets to business processes to value chains (cf. Section 5.3).

The assignment-concept—which can also be found to some extent in prior literature (Sienou et al. 2007; zur Muehlen and Rosemann 2005)—is refined in two ways. First, one can imagine additional kinds of relationships between risks and between chances such as intensification, weakening, or compensation. Currently, such interactions are denoted in *description*, optionally enriched with a *probability* concerning the manifestation of this influence. Alternatively, such relationships can be realized by specializing the meta type *Assignment*. However, the domain analysis did not reveal further differences from a conceptual modeling perspective between a conceptualization in terms of attributes or of separate meta types. For that reason, and following the hypothesis devised above, we decided against specializing *Assignment* in order to reduce the burden on the user. Second, similarly to *Uncertainty*, *Assignment* provides means to annotate assumptions underlying the relationship as well as the confidence in the strength relationship as a descriptive text. Thus, the interdependencies between IT risks and between IT chances can be distinguished into (logic-based) causal relations, (empirically-statistically validated) correlations, and mere assumed relations.

The meta model in Figure 4 contains further meta types, including *OrganisationalRole* to represent organizational responsibilities for uncertainties and measures as well as a concept for measure itself. A measure represents an action that is undertaken in order to influence at least one uncertainty. In case of risks, a measure aims at mitigation, avoidance, or transfer (Gemmer 1997; Heemstra and Kusters 1996); in case of chances, a measure is an action that aims to facilitate its realization. *Measure* comprises the attributes *implementationType* (e.g., 'manual' or 'automated') and *actionType* (point in time of application; e.g., 'proactive' or 'reactive'). To support cost-benefit analyses of measures (in terms of avoided/reduced risks) and analyses about the economic preferability of different measures having a similar impact on uncertainties, *Measure* is associated with the meta type *Cost* (representing the costs that incur for their implementation), *MeasureImpact* (describing a measure's impact on an uncertainty), and *MeasureRelationship*. The impact of measures can be characterized by a direction (positive/negative) and if needed a probability of whether the effect appears. Similarly to *Assignment*, a measure can have an impact on an uncertainty either individually or as a composite (expressed by the *1..** cardinality at *Measure*). The different relationships between measures (e.g., substitution, requirement, or support) are subsumed under *MeasureRelationship*. As with *Assignment,* we decided against a further differentiation through specialized meta types. Figure 6 illustrates key notational elements for the main concepts of RISKML.

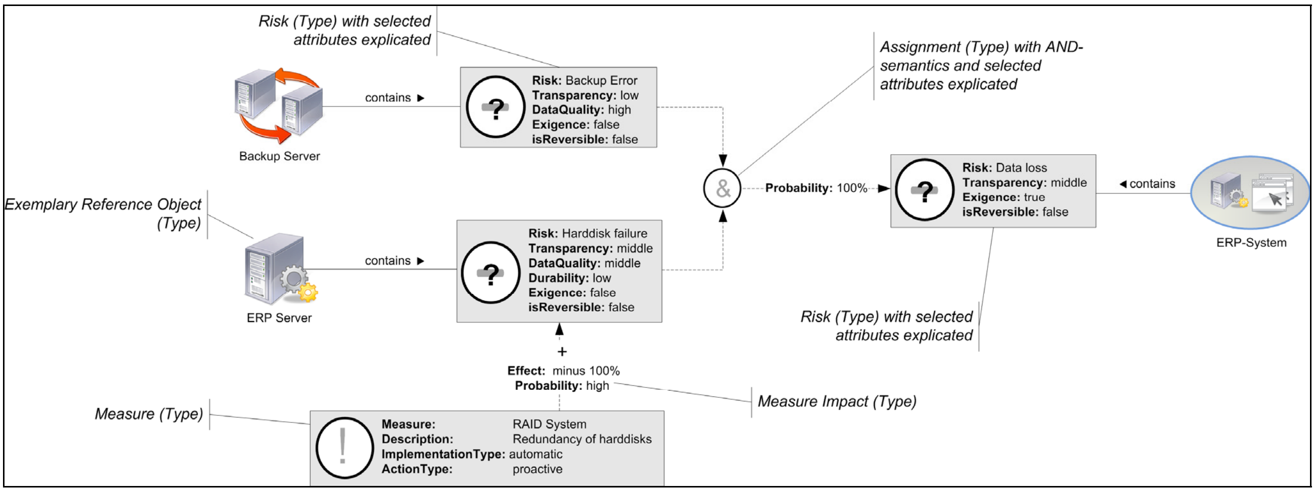

Figure 6 – Notational elements for key concepts and their relationships

5.3 The MEMO Risk Process Model

A process model, RISKPM, accompanies the RISKML to guide development and utilization of models to support IT risk assessment. The RISKPM covers the three main IT risk assessment phases—risk identification, risk analysis, and risk prioritization—that precede the actual risk management process (cf. *Requirement 6*).

Risk Identification

Risk identification is concerned with identifying IT risks and IT chances at those levels of the organization that seen as relevant to the analysis by the involved stakeholders. The primary objective is to identify *all* uncertainties *deemed as relevant* for the subsequent risk evaluation. RISKPM recommends starting the risk identification by analyzing existing enterprise models, because they should provide an overview of potential reference objects from which risks and chances originate and to which uncertainties are associated. Intuitively, a bottom-up approach starting with resource types or even instances of resources should quickly reveal key risk sources, perhaps a particular hardware or information system. Following Rainer et al. (1991), a complementary top-down approach starting with value activities at the strategy level is recommended so as not to overlook important risks and chances affecting value creation (and its potential destruction). Additionally, the identification of risks can be supported by a range of tools and techniques suggested in literature, like IT risk catalogues, prepared checklists, stakeholder questionnaires, and creativity techniques (Bandyopadhyay et al. 1999; Heemstra and Kusters 1996).

All identified uncertainties are represented using the language concepts of the RISKML. Identifying and annotating all reference objects associated with an uncertainty and documenting any remaining open issues in the model is recommended. Since the identification and description of an uncertainty often relies on subjective perception (cf. *Requirement 4*) and, hence, not necessarily on logic and factual reasoning (Clemen 1999; Klinke and Renn 2002), it is prudent to explicitly denote the assumptions, and possibly the objections, underlying the assessment of a particular stakeholder using the *assumption* attribute. This fosters the explicit consideration of divergent personal opinions of involved stakeholders and of (potential) resulting conflicts of interest. Specifically, it allows for assumption analyses as suggested by Remenyi et al. (2007). Figure 7 illustrates an outcome of the first step in the risk identification.

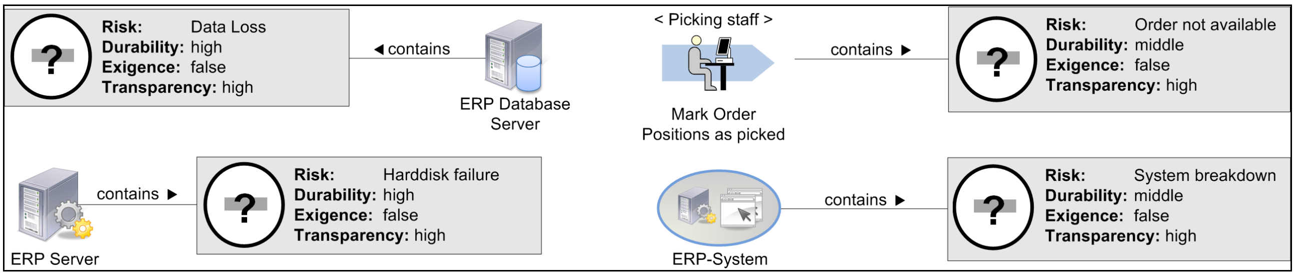

Figure 7 – Example of result of risk identification (singular risks)

After relevant IT risks and IT chances have been identified and initially documented, their effect relations have to be analyzed in order to prepare for a comprehensive assessment of risks and chances as well as for the evaluation and selection of adequate and economically reasonable measures. For this relationship analysis, we again suggest a combined top-down and bottom-up approach following (Neiger et al. 2006): Starting at the strategic level and gradually progressing further down the organizational levels, for each uncertainty its *causes* have to be identified (top-down). This requires an examination of uncertainties of (associated) reference objects at the level "beneath" the current reference object—for instance, uncertainties associated to hardware and software that constitute the information system that is currently under consideration. In the complementary bottom-up approach, the uncertainties on each level are analyzed for their *consequences* at the level above. The conceptual models support the search for effect relationships, and visualize dependencies between reference objects, such as 'comprises' or 'uses', between IT assets, processes and aggregated processes—and, thus, support an analysis of cause-and-effect relationships among these objects.

The identified cause-and-effect relations are modeled using the concept *Assignment*. Similar to the documentation of uncertainties, the underlying *assumptions* as well as the *maturity* of this relationship should be documented. Figure 8 shows an exemplary outcome of the second step of risk identification.

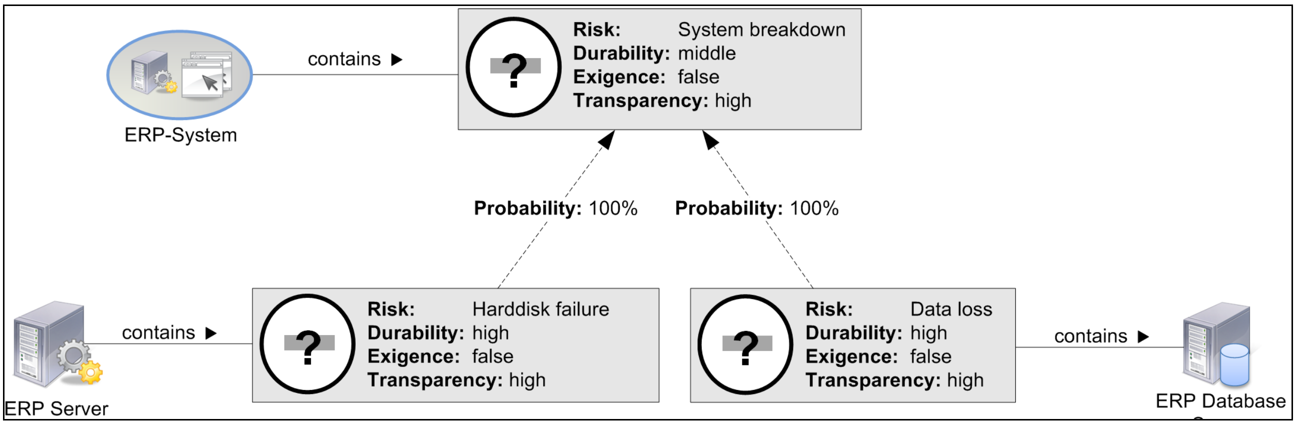

Figure 8 – Examples of result of risk identification (assigned risks)

Risk evaluation

Once the relevant uncertainties and their relations have been identified they can be evaluated. Risk evaluation means analyzing their effect in relation to corporate goals and usually consists of two aspects:

evaluating the probability and evaluating the impact. For each elementary uncertainty, or each uncertainty that is not associated with a cause, a probability has to be estimated and documented (using *EffectSpecification*). Thereafter, the probabilities of the associated consequences can be calculated – for instance, by aggregation rules the stakeholders involved have previously agreed on (in the case of textual or ordinal values), or by statistical methods (Chavez-Demoulin 2006; Clemen 1999).

Since the relationships among uncertainties are visually represented in the models, the effects of an uncertainty on a lower organizational level can be traced up to the strategic level. This allows evaluation of the effects of an uncertainty at IT operations level on business processes and corporate goals. Risk evaluation techniques involving stakeholders at different organizational levels (e.g., group discussions) are thereby supported by the different levels of abstractions the method provides.

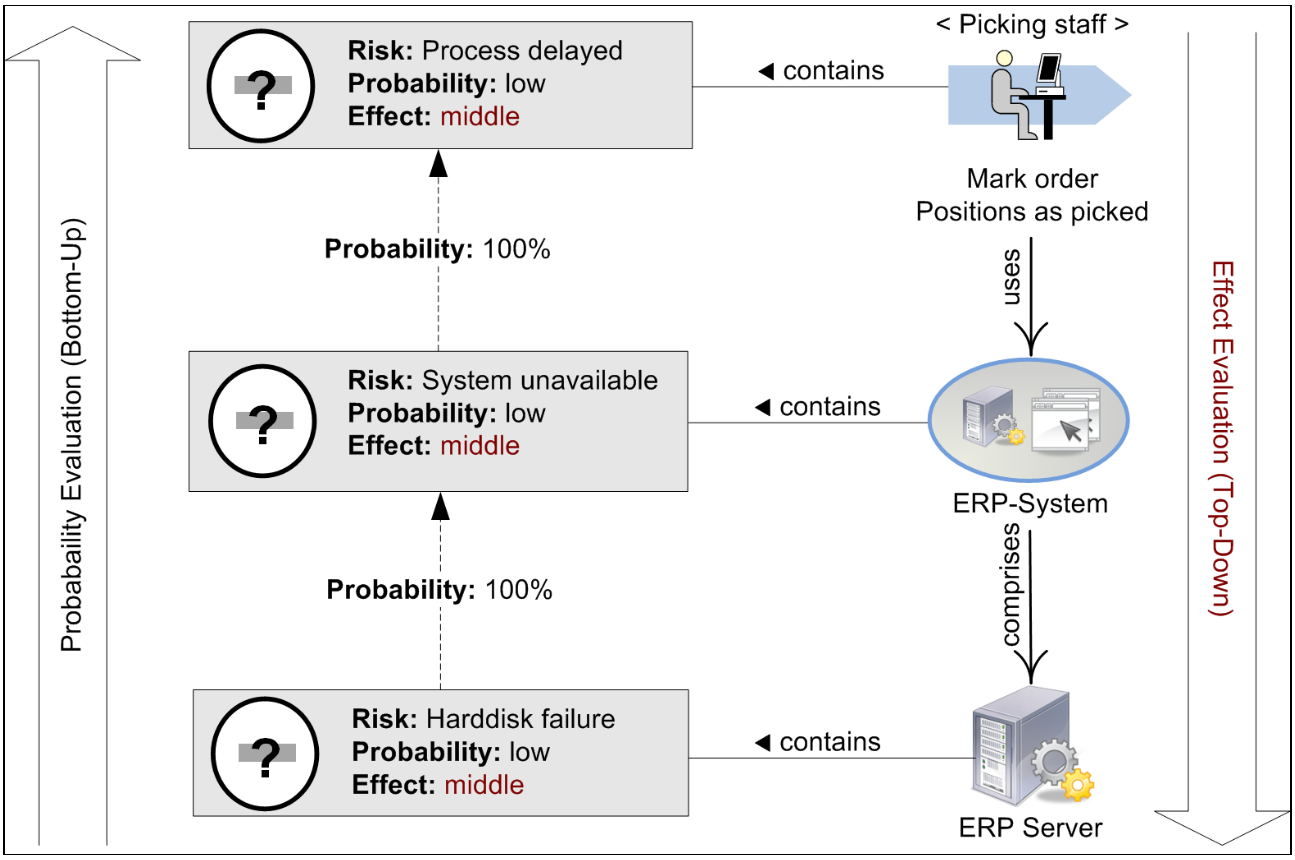

Figure 9 – Recommended procedures for risk evaluation

In contrast to the probability, the impact is evaluated top-down, starting from effects of an uncertainty at strategic level down to the effects of its causes at IT operations level. We assume that the evaluation of the impact of an uncertainty at IT operations level can be improved if its effects on other organizational levels are taken into account as well. Further, in the case of quantifications of IT-related risks and chances on a monetary scale, instruments such as (reciprocal) Time Savings Time Salary (Boczany 1983) and Functional Analysis of Office Requirements (Schaefer 1988)—which both apply at the business process level—are supported. Note that often the evaluation of probabilities or impact has to be conducted in an iterative fashion (Remenyi et al. 2007, p. 160). Figure 10 provides an example of risk evaluation and the corresponding utilization of enterprise models.

Risk prioritization

Finally, uncertainties have to be prioritized in order to decide on their effective relevance given the particular risk management situation, and following that, decisions have to be made on their treatment and then appropriate measures have to be agreed and implemented. The priority of an uncertainty is typically derived through quantitative assessment, usually based on probability and impact, and, hence, is not provided as a dedicated meta attribute. Given the semi-formal specification of the MEMO family of modeling languages, the transformation of model elements to other visual representations commonly used for risk prioritization (e.g. Ishikawa diagrams) can be at least partially automated. For each uncertainty, available measures can be annotated (cf. Figure 6). Assuming that their implementation costs are estimated, cost-benefit analyses, and analyses of how advantageous different measures are, prove to be feasible based on the risk models. The presented RISKPM focuses on supporting a generic IT risk assessment process. However, it can be adapted to support further decision scenarios, for instance, as part of make-or-buy decisions on specific IT assets or to analyze the economic efficiency of information systems, including costs, benefits—and risks—at different organizational levels.

6. Method Evaluation

The three design goals stated in Section 1, fostering communication and collaboration, reducing complexity, and improving transparency of IT risk matters, are refined and operationalized through the six requirements. The method evaluation assumes that by satisfying these requirements, the design goals are met. In turn, this implies that hypotheses underlie the relationships between high-level and low-level requirements. It is, for example, assumed that if a method supports integrated perspectives tailored to the needs of stakeholders involved in IT risk assessment (cf. *Requirement 1*), communication barriers are lowered and collaboration among stakeholders with different professional backgrounds is facilitated. In other words, the method positively contributes to approaching the primary design goal (Figure 10 provides an illustrative example of different perspectives provided by RISKM). The remaining hypotheses are interpreted accordingly but not made explicit, since the presumed effect and its direction can be inferred from Section 3.

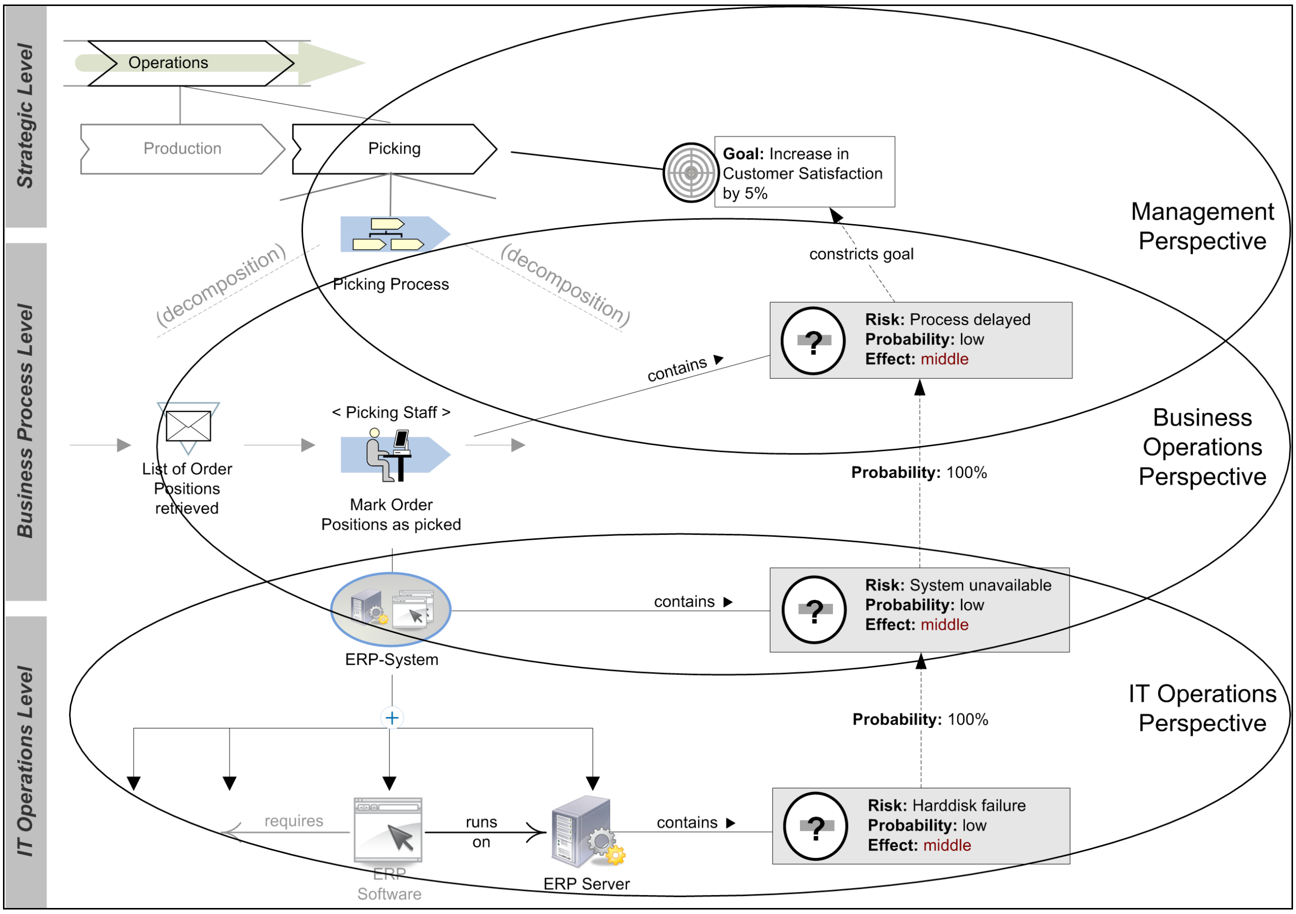

Figure 10 – Support for different perspectives for IT risk assessment (based on Figure 3)

Table 2 reviews how the RISKM method addresses the six requirements. RISKM addresses all requirements except for *Requirement 5*. In contrast to Sadiq et al. (2007), RISKML does not provide dedicated concepts to represent internal controls and, hence, RISKM does not support compliance validation for auditing purposes. A closer inspection of how RISKM addresses the requirements directs the focus to the domain-specific concepts provided by RISKML (cf. Table 3). The language specification accounts for both IT risks and chances and proposes uncertainty as an abstraction over the two types, so as to offer a solution to the terminological ambiguities of the domain (cf. *Requirement 2*).

Table 2: Evaluation of requirements

Requirement #	Description	RiskM
Requirement 1 *Multiple Perspectives*	A method should provide perspectives specific to (groups of) stakeholders involved in the group process. A perspective should, as far as possible, correspond with the abstractions, concepts and (visual) representations known and meaningful to the targeted (group of) stakeholders. All perspectives should, on the other hand, be integrated with each other to foster cross-perspective communication and cooperation.	Reconstruction of domain-specific concepts in meta model; Reuse of concepts provided by MEMO to tailor perspectives to needs of stakeholders; Integration through common meta and meta-meta models
Requirement 2 *Organizational Context*	A method should account for both IT-related risks and chances and link them to the surrounding action system comprised of all relevant organizational entities such as corporate goals, organizational units, and business processes.	Reconstruction of key concepts in meta model; Reuse of concepts provided by MEMO to provide organizational context
Requirement 3 *Multiple Organizational Levels*	A method should account for cause-and-effect relationships of IT risks and chances at multiple organizational levels, from IT operations to business processes to effects on value chains and the organization as a whole.	Reconstruction of key relationships among concepts in meta model; Reuse of concepts provided by MEMO to tailor organization levels to needs of stakeholders
Requirement 4 *Quantitative Values & Qualitative Descriptions*	A method should provide means for risk quantification where possible and means for qualitative risk description where quantification is either not feasible or not economically justifiable.	Introduction of concepts extending the domain terminology, e.g., attribute type *EffectSpecification*
Requirement 5 *Compliance*	A method should support compliance validation and auditing procedures, e.g., by representing the concepts built into regulations, standards and frameworks such as COBIT, or by (possibly partially automated) validation of internal controls.	Not supported
Requirement 6 *Multiple Phases*	A method should account for the multiple phases of the IT risk assessment process and facilitate transitions between phases, e.g., from IT risk identification to risk analysis.	Internally by choosing phase-specific modeling concepts; externally through model transformations, e.g., into other representations and diagram types

It is, however, important to recall the focus on downside risk in common business practice. An assumption associated with the present conceptualizations in RISKML is that the additional semantics of concepts defined by their attributes and relationships promotes comprehension by prospective users. Further research has to study the effects of the presented conceptualizations on prospective users, i.e., whether the proposed concepts indeed improve communication and cooperation or whether their graphical representations are accepted by the stakeholders involved in IT risk assessment.

Table 3: Key domain-specific concepts in RISKML

Key concept	RISKML
Risk / Chance / Uncertainty	*Uncertainty* as generalization of *risk* and *chance*; additional semantics through attributes
Goal	Explicitly modeled as goal and strategy models (Frank and Lange 2007)
Reference Objects	IT assets, business processes, value chain, among others
Assumptions	Explicitly both for uncertainties and assignments of uncertainties
Quantification/ Qualification	Attribute type *EffectSpecification* supports both
Measure	*Measure* as abstraction over various risk treatment strategies
Relationships	*Generalization*, *Aggregation*, *Cause-Effect-Relationship*, as well as *Risk-Chance-Relationship*
Organizational Role	Explicitly modeled as organizational role
Control	—
Metric	Indirectly as cost of a measure; explicitly due to integration with MEMO Score-ML (Frank et al. 2008)

With respect to the other conceptualizations, it has to be noted that some concepts in RISKML reconstruct common domain terminology and semantics, for example, probability and impact with respect to risk quantification. Other concepts, such as assumptions underlying risk quantification and qualification, have been discussed in the domain but may not be widely used in practice. With respect to these concepts, it is assumed that RISKML also frames a space for potential extensions to current business practice that contributes to the goal of increased transparency and traceability, in that explicitly modeling assumptions allows investigation of why a specific risk constellation was assessed in a particular way. The number of concepts and the diversity of relationship types in RISKML (e.g., between uncertainties of the same type and of different types and associations with a range of reference objects) suggests that the language itself increases complexity when using the method. It is thus currently not feasible to reason about the effects of RISKM on the complexity-reducing effects of using a DSML in IT risk assessment and the complexity-increasing effects of the method itself. Further research is needed to investigate these two opposing effects.

A further limitation of the proposed method pertains to its supposedly high costs due to demanding skill, know-how, and time requirements. These costs should decline (1) as reference models for IT risks (i.e. models of certain resource types enriched with typical risks) become available, so that model reuse increases and modeling efforts reduce; (2) if risk modeling is conducted as part of other modeling activities in the context of business process management (Sienou et al. 2008), so that existing models and know-how can be reused; (3) if a proper level of detail in the effect specifications of risks is chosen for IT risk assessment; and (4) if modeling tool support becomes available.

7. Conclusion

This research was conducted following a design research process (Verschuren and Hartog 2005) configured for the epistemological particularity of research on modeling methods (Frank 2006) to develop a linguistic artifact—a multi-perspective modeling method—that supports communication and collaboration among the various stakeholders involved in IT risk assessment. The method consists of a domain-specific modeling language, its graphical notation, and a corresponding process model that guides their application along the IT risk assessment lifecycle. It is built upon and extends an enterprise modeling approach to benefit from the reuse of modeling concepts to provide multiple perspectives on IT risk matters and on relevant organizational context. Using a prototypical application scenario, the study demonstrates how the method supports IT risk identification, analysis, and prioritization. Results of the method evaluation, which discussed method features in the light of essential domain-specific requirements and prior work, showed that the presented multi-perspective modeling method meets five essential domain-specific requirements of an IT risk assessment method and provides syntax and semantics of dedicated modeling constructs for key domain-specific concepts. The findings indicate that its graphical notation and meta model-based specification allows the convenient creation of consistent IT risk models that promise to facilitate interpretation and assessment of IT risk matters in group processes. This finding also contributes to existing literature related to conceptual modeling of IT risk matters in that it adds further semantics to key modeling concepts and frames a space for potential extensions to current business practice (e.g. by modeling assumptions underlying relationships among risks and processes) that contributes to the goal of increased transparency and traceability. Besides IT risk assessment group processes, the method supports additional analyses, for example, query a repository of identified IT risks and chances for analytical and for decision-making purposes. The chosen approach of domain-specific modeling also permits the transformation of IT risk models to generate code, for instance, a database schema, thus supporting the development of corresponding IT risk management systems. In this regard, the artifact outlined in the paper marks a further step towards a more comprehensive modeling method for governance, risk, and compliance (GRC) applications in information systems. Such a method remains on our research agenda.

Acknowledgement

The authors would like to thank the anonymous referees for their constructive comments that greatly helped improve the paper. We would also like to thank Arne Weuster for his support and Jens Gulden for valuable comments on an earlier version of the manuscript.

References

Atkinson, C., & Kuehne, T. (2008). Reducing accidental complexity in domain models. *Software and Systems Modeling*;7(3), 345–359.

Bandyopadhyay, K., Mykytyn, P. P., & Mykytyn, K. (1999). A framework for integrated risk management in information technology. *Management Decision*;37(5), 437–444.

Boczany, W. J. (1983). Justifying Office Automation. *Journal of Systems Management*;34(7), 15–19.

Carnaghan, C. (2006). Business process modeling approaches in the context of process level audit risk assessment: An analysis and comparison. *International Journal of Accounting Information Systems*;7(2), 170–204.

Chavez-Demoulin, V., Embrechts, P., Neslehova, J. (2006). Quantitative models for operational risk: Extremes, dependence, and aggregation. *Journal of Banking and Finance*;30(10), 2636–2658.

Clemen, R. T., Winkler, Robert L. (1999). Combining Probability Distributions From Experts in Risk Analysis. *Risk Analysis*;19(2), 187–203.

Crouhy, M., Galai, D., & Mark, R. (2001). *Risk management*. New York: McGraw-Hill.

Davies, I., Green, P., Rosemann, M., Indulska, M., & Gallo, S. (2006). How do practitioners use conceptual modeling in practice? *Data & Knowledge Engineering*;58(3), 358-380.

Frank, U. (1994). *Multiperspektivische Unternehmensmodellierung: Theoretischer Hintergrund und Entwurf einer objektorientierten Entwicklungsumgebung*. München: Oldenbourg

Frank, U. Conceptual Modelling as the Core of the Information Systems Discipline - Perspectives and Epistemological Challenges *Proceedings of the Proceedings of the Fifth Americas Conference on Information Systems (AMCIS 99)*, Milwaukee, WI, 1999, 695-697.

Frank, U. Multi-perspective enterprise modeling (MEMO): Conceptual framework and modeling languages *Proceedings of the Proceedings of the 35th Annual Hawaii International Conference on System Sciences (HICSS).* Honululu, 2002, 72–82.

Frank, U. (2006). *Towards a Pluralistic Conception of Research Methods in Information Systems Research*. Institute for Computer Science and Business Information Systems (ICB), Duisburg-Essen University. ICB Research Report 7.

Frank, U. (2008). *The MEMO Meta Modelling Language (MML) and Language Architecture*. Institute for Computer Science and Business Information Systems (ICB), Duisburg-Essen University. ICB Research Report 24.

Frank, U., Heise, D., Kattenstroth, H., Ferguson, D., Hadar, E., & Waschke, M. ITML: A Domain-Specific Modeling Language for Supporting Business Driven IT Management. In Rossi M, Gray J, Sprinkle J, Tolvanen J-P, eds. *Proceedings of the 9th Workshop on Domain-Specific Modeling (DSM) at the International Conference on Object Oriented Programming, Systems, Languages and Applications (OOPSLA)*, Orlando, Florida, USA, 2009.

Frank, U., Heise, D., Kattenstroth, H., & Schauer, H. Designing and Utilising Business Indicator Systems within Enterprise Models - Outline of a Method. In Loos P, Nüttgens M, Turowski K, Werth D, eds. *Proceedings of the Modellierung betrieblicher Informationssysteme (MobIS 2008)*, Saarbruecken, Germany, 2008, Koellen:89-105.

Frank, U., & Lange, C. (2007). E-MEMO: a method to support the development of customized electronic commerce systems. *Information Systems and E-Business Management*;5(2), 93–116.

Gemmer, A. (1997). Risk Management: Moving Beyond Process. *Computer*;30(5), 33–43.

Gerber, M., & Solms, R. v. (2005). Management of risk in the information age. *Computers & Security*;24(1), 16–30.

Hatfield, A. J., Hipel, Keith W. (2002). Risk and Systems Theory. *Risk Analysis*;22(6), 1043–1057.

Heemstra, F. J., & Kusters, R. J. (1996). Dealing with risk: a practical approach. *Journal of Information Technology*;11, 333–346.

Kirchner, L. Cost Oriented Modelling of IT-Landscapes: Generic Language Concepts of a Domain Specific Language. In Desel J, Frank U, eds. *Proceedings of the Proceedings of the Workshop on Enterprise Modelling and Information Systems Architectures (EMISA 2005)*, 2005, 166–179.

Kliem, R. L. (2000). Risk Management for Business Process Reengineering Projects. *Information Systems Management*;17(4), 71–73.

Klinke, A., & Renn, O. (2002). A New Approach to Risk Evaluation and Management: Risk-Based, Precaution-Based, and Discourse-Based Strategies. *Risk Analysis*;22(6), 1071–1094.

Lankhorst, M. (2005). *Enterprise Architecture at Work : Modelling, Communication and Analysis*. Berlin: Springer.

Loch, K. D., Carr, H. H., & Warketin, M. E. (1992). Threats to Information Systems: Today's Reality, Yesterday's Understanding. *MIS Quarterly*;16(2), 173–186.

Lu, R., Sadiq, S., & Governatori, G. Compliance Aware Business Process Design. In Hofstede AHMt, Benatallah B, Paik H-Y, eds. *Proceedings of the Business Process Management Workshops*, Brisbane, 2008, Springer:120–131.

March, J. G., & Shapira, Z. (1987). Managerial perspectives on risk and risk taking. *Manage. Sci.*;33(11), 1404–1418.

McGaughey Jr., R. E., Synder, C. A., & Carr, H. H. (1994). Implementing information technology for competitive advantage: Risk management issue. *Information & Management*;26(5), 273–280.

Mun, J. (2004). *Applied risk analysis : Moving beyond uncertainty in business*. Hoboken, NJ: John Wiley & Sons.

Neiger, D., Curilov, L., zur Muehlen, M., & Rosemann, M. Integrating Risks in Business Process Models with Value Focused Process Engineering *Proceedings of the Proceedings of the 2006 European Conference on Information Systems (ECIS 2006), Goteborg, Sweden, June 12-14, 2006*, 2006.

Odell, J. (1998). Power Types. In Odell J, ed. Advanced Object-Oriented Analysis and Design Using UML, (1998). Cambridge: Cambridge University Press.23–33.

Rainer, R. K., Synder, C. A., & Carr, H. H. (1991). Risk Analysis for Information Technology. *Journal of Management Information Systems*;8(1), 129–147.

Remenyi, D., Bannister, F., & Money, A. (2007). *The Effective Measurement and Management of ICT Costs & Benefits*. Oxford: Elsevier.

Rogers, S., Lukens, S., Lin, S., & Jon, E. (2008). *Balancing Risk and Performance with an Integration Finance Organization (The Global CFO Study 2008)*. Somers, NY: IBM Global Business Services.

Sadiq, S., Governatori, G., & Namiri, K. Modeling Control Objectives for Business Process Compliance. In Alonso G, Dadam P, Rosemann M, eds. *Proceedings of the Business Process Management*, 2007, Springer:149–164.

Salmela, H. (2008). Analysing business losses caused by information systems risk: a business process analysis approach. *Journal of Information Technology*;23(3), 185–202.

Sayer, P., & Wailgum, T. (2008). What You Can Learn about Risk Management from Société Générale. http://www.cio.com/article/336816/What_You_Can_Learn_about_Risk_Management_from_Societe_Generale. Accessed Jan 21, 2009.

Schaefer, G. (1988). *Functional Analysis of Office Requirements: A Multiperspective Approach*. Chichester: Wiley.

Scheer, A.-W. (1992). *Architecture of Integrated Information Systems : Foundations of Enterprise Modelling*. Berlin ; New York: Springer.

Scheer, A.-W. (1999). *ARIS - Business Process Frameworks*. 3. ed. Berlin: Springer.

Scheer, A.-W. (2000). *ARIS - Business Process Modeling*. 3. ed. Berlin, Heidelberg: Springer.

Schelp, J., & Winter, R. Method Engineering: Lessons Learned from Reference Modeling. In Chatterjee S, Hevner A, eds. *Proceedings of the First International Conference on Design Science Research in Information Systems and Technology (DESRIST'06)*, Claremont, CA, 2006.

Sienou, A., Lamine, E., Karduck, P. A., & Pingaud, H. Conceptual model of risk: towards a risk modeling language. In Weske M, Hacid M-S, Godart C, eds. *Proceedings of the Proceedings of Web Information Systems Engineering – WISE 2007 Workshop*, Montpellier, France, June 17, 2008, 2007, Springer:118–129.

Sienou, A., Lamine, E., & Pingaud, H. A Method for Integrated Management of Process-risk. In Sadiq S, Indulska M, zur Muehlen M, Franch X, Hunt E, Coletta R, eds. *Proceedings of the Proceedings of the 1st International Workshop on Governance, Risk and Compliance - Applications in Information Systems (GRCIS'08) held in conjunction with the CAiSE'08 Conference*, Montpellier, France, June 17, 2008, 2008.

Verschuren, P., & Hartog, R. (2005). Evaluation in Design-Oriented Research. *Quality & Quantity*;39(6), 733-762.

Wand, Y., Monarchi, D. E., Parsons, J., & Woo, C. C. (1995). Theoretical foundations for conceptual modelling in information systems development. *Decision Support Systems*;15(4), 285-304.

Wand, Y., & Weber, R. (2002). Research Commentary: Information Systems and Conceptual Modeling-A Research Agenda. *Information Systems Research*;13(4), 363-376.

Ward, S., & Chapman, C. (2003). Transforming project risk management into project uncertainty management. *International Journal of Project Management*;21(2), 97-105.

Weill, P., & Ross, J. W. (2004). *IT Governance: How Top Performers Manage IT Decision Rights for Superior Results*. Harvard Business School Press.

Westerman, G., & Hunter, R. (2007). *IT Risk: Turning Business Threats into Competitive Advantage*. Cambridge: Harvard Business School Press.

Willcocks, L., & Margetts, H. (1994). Risk assessment and information systems. *European Journal of Information Systems*;3(2), 127-138.

zur Muehlen, M., & Rosemann, M. Integrating Risks in Business Process Models *Proceedings of the Proceedings of the 16th Australasian Conference on Information Systems (ACIS 2005)*, Sydney, 2005, 62-72.

Authors biographical information

Stefan Strecker is currently an assistant professor at the Institute for Computer Science and Business Information Systems, University of Duisburg-Essen, Germany. He received his doctorate from the Department of Economics and Business Engineering at Universität Karlsruhe (TH), Germany. Currently, he is working towards his post-doctoral thesis, 'Habilitation' . Dr. Strecker has published in *Decision Support Systems*, *Business & Information Systems Engineering*, *Enterprise Modelling and Information Systems Architectures*, *Group Decision and Negotiation*, and several conference proceedings. His current research interests include enterprise modeling, IS assessment, and electronic negotiations. He can be reached at stefan.strecker@uni-due.de.

David Heise is currently a doctoral candidate at the Institute for Computer Science and Business Information Systems, University of Duisburg-Essen. He received his undergraduate and graduate degrees in Information Systems from the Department of Economics and Business Administration at Duisburg-Essen University. David Heise has published in several conference proceedings and received the David-Kopf-Award 2008 for his graduate thesis. His current research interests include enterprise modeling, IS management, and IS assessment. He can be reached at david.heise@uni-due.de.

Ulrich Frank is Professor of Information Systems and Enterprise Modeling at the Institute for Computer Science and Business Information Systems, University of Duisburg-Essen, Germany where he heads the Enterprise Modeling research group. Prof. Frank has published in German and international journals, monographs, and book chapters. He is Editor-in-Chief of *Enterprise Modelling and Information Systems Architectures* and serves on the editorial boards of *Information Systems and E-Business Management*, *Business & Information Systems Engineering* and its German sibling, *WIRTSCHAFTSINFORMATIK*. His research focuses on the design and evaluation of languages and methods for multi-perspective enterprise modeling. In addition, his research topics include software engineering, IS management, and the philosophy of science. He can be reached at ulrich.frank@uni-due.de.