Toward modeling constructs for audit risk assessment: Reflections on internal controls modeling

Stefan Strecker, David Heise, Ulrich Frank

Information Systems and Enterprise Modelling Research Group
Institute for Computer Science and Business Information Systems
University of Duisburg-Essen, Universitaetsstr. 9, 45141 Essen, Germany
{stefan.strecker | david.heise | ulrich.frank}@uni-due.de

Abstract: Auditors face a number of challenges when performing audit risk assessment. To cope with these challenges, methods are required that purposefully reduce the complexity inherent to internal control systems and that facilitate communication about internal control matters among groups of stakeholders with differing perspectives on the subject matter. In this paper, we investigate the potentials of an enterprise modeling approach to audit risk assessment and propose conceptualizations for modeling constructs as enhancements to enterprise modeling to support audit risk assessment.

Keywords: Enterprise modeling; Language design; Internal controls; Audit risk assessment; Governance, Risk, Compliance

1 The extended scope of audit risk assessment

Section 404 of the Sarbanes-Oxley-Act of 2002 (SOX) and both the Directives 2006/43/EC and 2008/30/EC of the European Parliament and of the European Council ("EuroSOX") mandate the establishment, documentation and management of internal control systems and their subsequent auditing as part of audit risk assessment. Present auditing standards and guidelines commit auditors to gain an in-depth understanding of a firm's business, its operations and processes, associated risks and internal controls when assessing the risk of material misstatement [SP02]. As relevant risks pervade the enterprise from operations to corporate strategizing, it needs to be questioned "[w]hy limit the analysis to the business process level?" [Dun06, 207]—when legal regulations and auditing standards prescribe assessing risks at all relevant levels of the organization [The92, Inf09]. Audit risk assessment therefore pertains to any risk of not achieving objectives not only risks related to financial reporting [CS02]. Hence, auditing standards "emphasize the importance of auditors gaining a broader understanding of an organization" [Car06, 171]. Put differently, auditing guidelines prescribe to account for the appropriate organizational context of internal controls: Auditors are required to understand a firm's business, its risks and controls in place to treat risk exposure at all relevant organizational levels which implies an understanding of entity objectives, business processes, organizational structures, roles, responsibilities and resources.

Against this background, auditors face a number of challenges when performing audit risk assessment: They are confronted with the remarkable complexity of present day enterprises—especially considering the multifaceted interrelations between organizational structures, business processes, and IT assets. Auditors also have to deal with the complexity of internal control systems themselves: Controls occur for multiple organizational levels, refer to a multitude of different entities and address a variety of risks—apart from the sheer number of controls and their possible interactions [Mai00]. Moreover, auditing internal control systems requires the participation of stakeholders with different professional backgrounds and perspectives on internal control matters including executives, line managers, process owners, risk managers, internal and external auditors [SP02]. In this respect, the complexity challenge is intensified by different technical languages, differing mindsets, and resulting barriers to communicate and to participate—hampering in particular the collaboration between auditor and auditee.

To cope with these challenges, methods are required that purposefully reduce the complexity inherent to internal control systems and that facilitate communication about internal control matters among groups of stakeholders The auditing and accounting literature recognizes the potentials of supporting audit risk assessment through conceptual models, in particular business process models in the context of process-level audit risk assessment (e.g. [Inf09, 132]). It is, however, acknowledged that present generic approaches to business process modeling do not provide adequate modeling constructs required for representing internal control systems with regard to effectively and efficiently supporting auditors when performing audit risk assessment [Car06]. In particular, it is criticized that present approaches focus on the business process level and do not provide support for adequately representing further relevant organizational context such as objectives, organizational roles, responsibilities and resources [Dun06]. Such modeling concepts are, however, common to enterprise modeling approaches such as ARIS [Sch00, Sch92], MEMO [Fra08, Fra02] and ArchiMate [Lan05] which supplement business process models with further abstractions of the enterprise (e.g. corporate goals and strategies, organizational structures, roles and resources). While current enterprise modeling approaches, thus, provide support for necessary organizational context, they—to our knowledge—do, however, not provide elaborate domain-specific modeling concepts for internal controls modeling.

In this respect, our motivation is twofold: We investigate the potentials of an enterprise modeling approach to audit risk assessment and propose conceptualizations for modeling constructs as enhancements to enterprise modeling approaches to support audit risk assessment. Next, we briefly review related literature (Section 2). Section 3 analyses and reconstructs technical terminology in the auditing domain. Section 4 introduces design goals and requirements a method for audit risk assessment should satisfy. The general prospects of an enterprise modeling approach to audit risk assessment are investigated in Section 5. In Section 6, we reflect on the design of domain-specific modeling constructs and discuss design issues. Section 7 presents concluding remarks.

2 Related work

Since McCarthy's work on the REA (resources, events, agents) model [McC79, McC82], auditing and accounting information systems literature recognizes the use of conceptual models of the enterprise for supporting accountants and auditors in understanding a firm's business [GSF04, DCH05, RBGR06]. Studies on the actual use of graphical representations support anecdotal evidence that system flowcharts and data flow diagrams are still the predominant means of graphical representation used in audit reviews [GSF04, 24]. A recent study shows, however, that business process modeling approaches such as the Business Process Modeling Notation (BPMN) or the Event-driven Process Chain (EPC) approach are gaining increasing acceptance in the auditing domain [ABC08]. At the same time, behaviorist research indicates that graphical representations of the enterprise advance the understanding of auditors over text-based documentation [ALM02, ABC04].

Carnaghan reviews different business process modeling approaches with regard to their support for audit risk assessment and concludes that present approaches do not allow for adequately expressing the semantics of internal controls and, consequently, further modeling constructs are required that explicitly capture the domain's technical language [Car06]. Dunn, in a review of the study, supports her conclusion by stating that "these tools were not designed with audit risk assessment suitability in mind but that is not to say that we couldn't develop one" [Dun06, 207]. This assessment, however, ignores contributions from the conceptual modeling community to the auditing domain.

For instance, Petri nets have for long been discussed as a means to document business processes and corresponding internal controls [PP97, CL03]. More recently, several approaches based on formal logic interpret internal controls in terms of formalized rules for a business process' control flow [GHSW08, LSG08, SGN07, GMS06, NS07]. These approaches primarily target compliance checking based on automated reasoning. Technology-focused research is aimed at computer-assisted auditing. Agrawal ea. [AJKL06], for instance, present a workflow engine that compares logs of process executions with predefined workflow schemas with regard to violations of audit constraints. Karagiannis ea. [KMS07] present modeling tool support for business process compliance. A further stream of literature deals with conceptual models of risks and chances [SHF10, SLKP07]. For example, zur Mühlen and Rosemann [zMR05] extend EPC with modeling concepts for risk types and related diagram types.

In summary, a rich body of literature contributes to support audit risk assessment through conceptual models. However, prior work has not discussed differentiated domain-specific modeling concepts for internal controls modeling. It also does not deal with the reuse of concepts in the context of enterprise modeling and of extending present enterprise modeling approaches with domain-specific concepts for internal controls modeling. Present modeling support for audit risk assessment focuses on business process models and on formal representations of internal controls. This brief analysis of the current state-of-the-art in literature motivates our research on domain-specific modeling constructs for audit risk assessment.

3 Domain analysis

Designing domain-specific modeling concepts presupposes reconstructing key terms and their semantics in the targeted domain. Reconstruction of domain-specific concepts is an iterative process involving not only the mere identification of candidate classes, their attributes and relations. Rather, it requires, for instance, identifying and resolving terminological ambiguity and truncation, e.g., by introducing additional abstractions and by shaping their conceptualization. This implies (re-)interpretation of observed terms and their semantics to design abstractions suitable for intended purposes, analyses and possibly for further future applications. One widespread approach to conceptual reconstruction—the one we follow here—is to review, analyze and interpret pertinent literature in the field under consideration. This section summarizes key findings from the conceptual reconstruction of the technical terminology in the auditing domain, specifically in the context of audit risk assessment.

In auditing literature and practice, "control", "internal control", and "internal control system" are commonly used terms [Moe08]. Despite their proliferation, a lack of precise definition and understanding of even these key domain concepts has repeatedly been criticized [Mai00]. The term "control" is in fact subject to a considerable diversity of disciplines, for example, "management control, organizational control, internal controls, operational control and financial control, which all seem to revolve around the same concept" [RBGR06]. The auditing perspective on *internal* control is decisively influenced by the Committee of Sponsoring Organizations of the Treadway Commission (COSO) [The92, The04] and subsequent auditing standards such as the Public Company Accounting Oversight Board (PCAOB) Auditing Standard No. 5 (for a discussion see [RBGR06] and [Mai00]):

> "COSO defines internal control as a process, effected by an entity's board of directors, management and other personnel. This process is designed to provide reasonable assurance regarding the achievement of objectives in effectiveness and efficiency of operations, reliability of financial reporting, and compliance with applicable laws and regulations. [...] Internal control is not merely documented by policy manuals and forms. Rather, it is put in by people at every level of an organization. [...]" ([The10]; adapted from [The92]).

While this very broad conceptualization provides insights into essential domain-specific concepts (e.g., objectives, policy, reasonable assurance), it also points to (necessary?) terminological ambiguity: Internal control obviously denotes *not only* a process but covers both procedural aspects (e.g., people, processes) and structural aspects (e.g., policy, organizational structures). Surprisingly, neither risk nor control objectives are mentioned—yet both constitute essential concepts in the frameworks provided by COSO and by the Information Systems Audit and Control Association (ISACA). In a later framework, COSO consequently adapts the internal control definition to the broader context of risk management: "Enterprise risk management is a process, [...] designed to identify potential events that may affect the entity, [...] to provide reasonable assurance regarding the achievement of entity objectives" [The04].

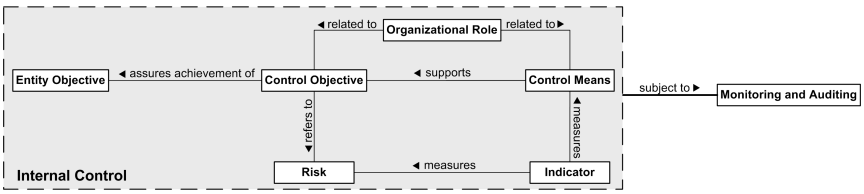


Figure 1: Initial reconstruction of domain terminology: Essential domain-specific concepts

Hence, in general, internal control can be said to refer to means to reduce risks of not achieving objectives [SP02]. Consequently, evaluation of internal controls by auditors is considered as a risk assessment process, often denoted as audit risk assessment. A first conclusion from this brief terminological analysis pertains to the very conception of "internal control": Internal control cannot be conceived as a singular concept as such, but rather as an abstraction over various other concepts which in turn constitute an internal control. An initial reconstruction of the constituent concepts of "internal control" is shown in Fig. 1. It is mainly based on an analysis of the mentioned COSO documentation, two textbooks [DCH05, GSF04] as well as anonymized audit documents received from a Big Four auditor.

A key domain concept is *control objective*, sometimes also denoted as control goal [GSF04, 249]. It represents a desired state of an enterprise ("Prevent unauthorized refunds") with respect to achieving an *entity objective* ("Minimize error rate of incorrect refunds") that is threatened by a *risk* ("Internal fraud due to fraudulent behavior of employees"). A control objective is associated with a recommended course of action that should be taken to provide reasonable assurance that entity objectives will be met and, thus, corresponding risks of not achieving it are mitigated. The course of action can involve policies, procedures, practices, or organizational structures as concrete measures or means of control implemented to ensure effectiveness of a control. A possible means to prevent fraud is "segregation of duties". Such a *control means* is aimed at achieving the control objective. It represents an abstraction over static means of control such as written policies or organizational structures and dynamic means of control such as activities and procedures. Alternative denominators to the control means concept could have been "control activity" [IT 07] and "control plan" [GSF04, 249]. Both, however, entail a significant risk of misinterpretation: The term "activity" raises associations with dynamic abstractions neglecting static aspects while the term "plan" emphasizes a perspective different from the intended means-end association. Examples for general control means given in COSO publications include the authorization of transactions as well as adequate safeguards of assets and records. The achievement of the desired outcome of a control objective is measured by an *indicator* (e.g., "Percentage of fraudulent refund transactions") as is the severity of risk. Responsibilities (as in the RACI conceptualization: "Responsible", "Accountable", "Consulted", "Informed") are defined typically for more than one *organizational role* ("executive", "business process owner", etc.) with respect to a control objective. It is important to note that frameworks such as the ones provided by COSO and the ISACA (e.g., COBIT) assume relationships between internal controls that typically form a hierarchy, possibly a net of controls. Also note that monitoring and auditing an internal control system (e.g., performed as audit risk assessment by an external auditor) constitute processes detached from the actual internal control system in that the system itself becomes subject to the audit [The09].

4 Design goals and requirements

The general purpose of this design research project is to effectively and efficiently support auditors when performing audit risk assessment. More specifically, this work is aimed at supporting auditors in understanding a firm's business, its operations and processes, associated risks and internal controls when assessing the risk of material misstatement. Given that the auditor's understanding is educed in group processes [Dam05, 79], its purpose is to support group processes by reducing the complexity inherent in internal control systems and by providing abstractions tailored to the perspectives of stakeholders involved. Thus, this work is aimed at fostering and facilitating communication and collaboration among stakeholders involved in audit risk assessment—with a dedicated focus on auditor and auditee interaction. It also aims to increase transparency of internal control matters, specifically by visually representing internal controls as part of the organizational action systems, and by improving traceability of the controls in place to treat risk exposure. Ultimately, this paper is also intended to intensify the dialog between the accounting information systems and the conceptual modeling communities.

The overall design goal is to enhance present enterprise modeling approaches by constructs for internal controls modeling. In this paper, however, we do not present a complete language specification but discuss design decisions and alternatives based on a preliminary draft of a language specification as an initial step toward developing modeling constructs for audit risk assessment. Below, we refine the stated purpose and goal to establish five domain-specific requirements that a method aimed at supporting audit risk assessment should satisfy (for a rationale also see [SHF10]).

Requirement 1—Organizational Context: A method should link internal controls to the surrounding organizational action system composed of all organizational entities relevant to audit risk assessment. This organizational context is provided by (at least) entity objectives, business processes, (IT) resources, organizational structures, roles and involvement.

Requirement 2—System of internal controls: A method should account for relationships among internal controls on different organizational levels, from IT operations to business processes to value chains to the organization as whole.

Requirement 3—Justification and assumptions: A method should provide means for justifying the existence and importance of internal controls and for revealing assumptions underlying internal control justification.

Requirement 4—Diversity of implementation: A method should account for the diversity of actual means to achieve control objectives and of the resulting internal control implementation.

Requirement 5—Support for 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.

5 Illustration of an enterprise modeling approach

This section illustrates the prospects of supporting audit risk assessment with domain-specific modeling concepts integrated with an enterprise modeling approach. The analysis is based on two presuppositions: First, we presume that the enterprise modeling method is based on a language architecture that allows for reuse of existing modeling concepts (for an example see [Fra08]). Second, we assume that the enterprise modeling method provides language concepts for representing control flows, goals, roles, and organizational structures as is the case, for instance, with ARIS [Sch00, Sch92] and MEMO [Fra08, Fra02]—thereby providing concepts to represent the organizational context required for internal controls (cf. Req. 1). The MEMO approach was chosen to illustrate the application scenario in Fig. 2, because it fulfills both assumptions and integrates further concepts essential to audit risk assessment (e.g., risk [SHF10], indicator [FHK09] and IT resources [Kir05]). It is important to note that the shown diagram is not intended to predetermine a specific language design. Instead, it serves as an illustration of principle applications of enterprise models in the context of audit risk assessment.

The scenario is based on and inspired by a business process model of a refunding returned goods process drawn on by [Car06, 200] to compare different business process modeling approaches in the context of audit risk assessment. The scenario shows a goal model (top left) that represents (an excerpt of) a hierarchy of the enterprise's strategic goals and subsequent business objectives; a business process model for "refunding returned goods" at three different levels of abstraction (i.e., an aggregated process and its decompositions; bottom left); a model of the corresponding organizational structure (including a model of organizational roles; top right) and a model of IT resources used in some of the processes (showing an information system abstraction of an ERP system; bottom right). Further models such as corresponding object models are not shown in the diagram for the sake of clarity. Relationships between concepts in different models are explicitly modeled by associations (e.g., the ERP system used in the business process "Authorize credit") or by shared concepts (e.g., the organizational role "A/R manager" in both the process "Authorize credit" and in the organizational structure model).

Provided such an infrastructure exists, internal controls modeling can be supported by extensions to existing concepts and by introduction of additional abstractions. We will illustrate the latter first. The scenario shown in Figure 2 assumes that some constituent concepts of internal controls are represented by *additional* modeling concepts. In particular, the control objective concept represents such an addition. The control objective "Prevent unauthorized refunds" recommends a segregation of duties in the aggregated process "Refund returned goods". The internal control semantics is further specified by the IT control "Prevent unauthorized transactions", by the risk "Internal fraud" it aims to mitigate, by the audit activity "Audit refund transactions and detect irregularity", and by the indicator "Percentage of fraudulent refund transactions" to measure achievement of the control objective. An *extension* to existing modeling concepts is shown as a visual overlay (a red triangle), which serves to highlight all those model elements that are related to an internal control. In Figure 2, for instance, the process "Authorize credit" is enriched with an overlay, as the process realizes a significant part of the segregation of duties. Similarly, overlays are

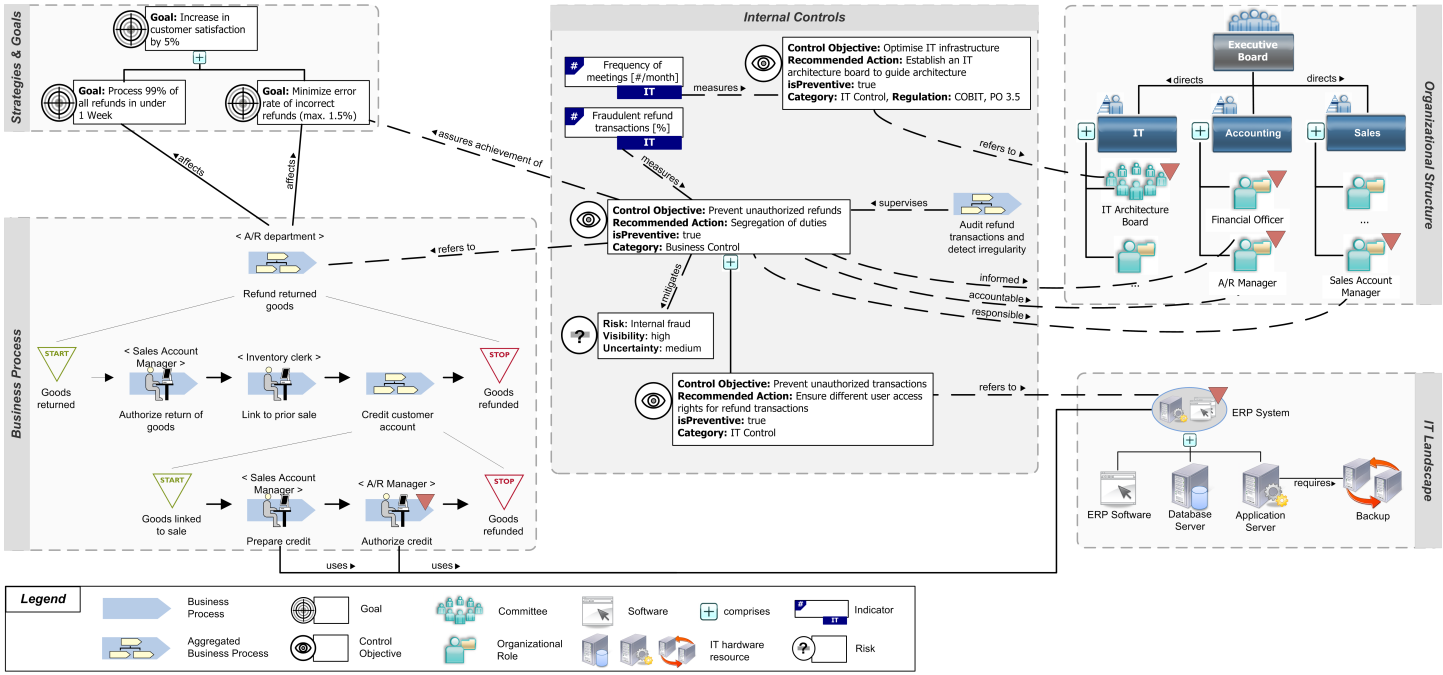


Figure 2: Illustration of an enterprise modeling approach to internal controls modeling

attached to the information system symbol “ERP system” in the IT landscape model and some of the organizational units in the structure model, since these elements are all related to the internal control(s).

Figure 2 also demonstrates how the control objectives can be associated with concepts that represent the organizational action system they are embedded in (cf. Req. 1). First, they can be associated to the entity objectives they are aimed at assuring the achievement of (i.e., the goal “Minimize error rate of incorrect refunds” in the goal model). Second, control objectives can be linked to static and dynamic abstractions representing means of control. For example, the above mentioned control objective refers to the business process “Refund returned goods”, whereas the actual realization of the recommended action “segregation of duties” is depicted at the most detailed level of the process model. Third, the IT control refers to an IT asset in the IT resource model (“ERP system”) that realizes the segregation at the information system level by authorization and system access policies. Linking the two control objectives also demonstrates how associations between controls aid in visualizing internal control systems. Finally, the integration with the model of the organizational structure emphasizes different types of involvement of organizational roles. For instance, the two roles participating in the “Credit customer account” process—“Sales Account Manager” and “A/R Manager”—are linked to the control objective specifying their type of involvement (i.e., ’accountable’ respectively ’responsible’), whereas a “Financial Officer” is regularly informed but not explicitly modeled as part of the business process.

With respect to the intended purpose of effectively and efficiently supporting auditors in understanding a firm’s business, its risks, and controls, such integrated models of the enterprise and its internal control system promise to provide an intuitive access and a comprehensible conceptual foundation for differentiated and structured analysis of the internal control system. By associating internal controls with further models (e.g., of business processes or IT landscapes) and by tagging affected reference objects with an overlay symbol, this approach facilitates internal control-related communication and collaboration between groups of stakeholders with different professional backgrounds (cf. Req. 5). By focusing on types (of controls, risks, processes etc.) rather than instances, such an approach purposefully reduces complexity and contributes to focusing on aspects relevant to the audit analysis.

Besides documentation—and thus queries on which controls exist in an enterprise—such integrated models support further analyses. On the one hand, they allow for analyzing controls in respect to the organizational context they affect. For instance, in Figure 2, the business control objective is associated to one of the firm’s business objectives, a business process, and an IT resource. For auditing purposes, this allows for comparing the current implementation of a control with, for instance, reference models of internal controls or check lists of prescribed control means. On the other hand, it allows for analyzing various organizational concepts with regard to whether they are affected by controls. Especially in organizational settings that experience rapid changes such an analysis can assist in preventing failure to comply with regulations. In Figure 2, for instance, an analysis of the committee “IT architecture board” reveals a relationship to a control objective, so that eliminating this organizational unit from the model (e.g., as a result of a reorganization project) raises an exception and notifies stakeholders of a likely compliance violation.

In summary, the illustrated enterprise modeling approach promises a number of advantages over textual representations, simple conceptual models or even present business process modeling approaches:

1. As a general prospect of enterprise modeling, the purposeful abstractions of the action system promise to reduce the complexity in analyzing a company's internal controls and, thus, per se announce support for internal and external auditors.
2. The proposed reuse of existing modeling concepts increases the productivity of both language design and language application. Language designers benefit from mature modeling concepts and notations and can focus on relevant additions and modifications. Modelers as language users benefit from the reuse of existing models (e.g., of business processes) and can focus on adding relevant contextual information (e.g., risks, indicators).
3. The partially formal specification of modeling concepts allows for model transformations into other representations (e.g., to some extent, into source code), which provides a foundation for developing corresponding information systems based on a model-driven development approach.
4. Reconstructing the technical terminology using such an enterprise model-based approach also carries the potential to contribute to a less ambiguous domain terminology (e.g., with respect to the term "internal control") in that it offers a conceptualization of key domain concepts with a partially formal semantics.

Based on these considerations, we envision that enterprise models enriched by dedicated internal control concepts can be used in audit reviews as audit evidence, i.e., as structured documentation of a firm's internal control system—to facilitate interpretation and assessment of controls by auditors.

6 Considerations on language design

Based on the corroborative assessment of the potentials of an enterprise modeling approach to audit risk assessment, this section outlines general considerations toward enhancing enterprise modeling approaches with domain-specific modeling concepts for audit risk assessment, and discusses essential decisions related to the design of these modeling constructs. In this section, we present preliminary specifications of modeling constructs as meta model excerpts specified using the MEMO Meta Modeling Language [Fra08]. These specifications are intended as a working draft for the following discourse and as a foundation for discussions with and discursive evaluation by peers and domain experts. In the following, we assume a modeling infrastructure as described in Sec. 5. The reuse of modeling concepts from existing modeling languages in the MEMO language family is visualized by a colored rectangle attached to the meta type header indicating the concept's origin (as suggested in [Fra08]).

6.1 Devising an infrastructure for internal controls modeling

Enhancing an enterprise modeling approach to support audit risk assessment requires conceptualizing modeling constructs based on domain-specific concepts. The initial design decision with respect to our targeted domain pertains to the conceptualization of an internal control. Based on the analysis in the previous sections, it appears justified to represent an internal control by its control objective and by the means of achieving the control objective. Hence, we decided to introduce two dedicated meta types, *ControlObjective* and *ControlMeans*. To represent the semantics of internal controls, further refinements are, however, necessary and detailed below. The rationale of introducing those two meta types is to enable dedicated audit analyses based on respective internal control models.

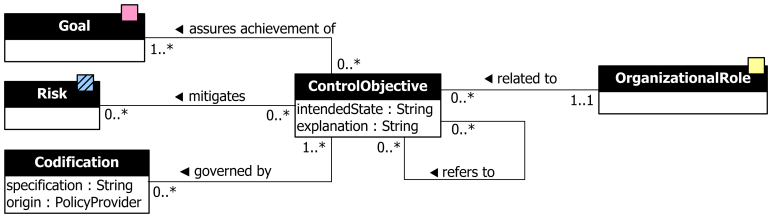


Figure 3: Conceptualization of "control objective"

ControlObjective. For conceptualizing the meta type *ControlObjective*, we propose to provide additional semantics by describing control objectives by a natural language specification of a desired state of the enterprise, for instance, by an attribute *intendedState* and an explanation of the intended state, *explanation*. Both attributes contribute to *Requirement 3—Justification and assumptions* in that they allow for providing a rationale for the existence and importance of an internal control. The importance of a control could have been further specified, for example, by an additional attribute, say priority. The present conceptualization subsumes this information under *explanation*. The justification is augmented by providing information on the *Codification* the control objective is governed by. In regard to the various legal regulations, auditing standards, and guidelines, feedback from practicing auditors revealed that it is recommended to keep track of these codifications (e.g. a certain clause in an auditing standard) and of the originating policy provider (e.g., COSO, PCAOB No. 5, COBIT). Note that in some cases it may be feasible to rephrase the natural language specification in a formal logic to support automated reasoning on control objectives (e.g., [SGN07]). In this respect, the proposed conceptualization simplifies future enhancements to cover such rule-based formalizations (e.g., as an additional attribute). The integration with an enterprise modeling approach allows to comfortably express further semantics of internal controls by associating the meta type *ControlObjective* to the meta types representing entity objectives (*Goal*), risks (*Risk*) and organizational structures (*OrganizationalRole*) and, thus, to promote reuse of modeling constructs and to address *Requirement 1—Organizational context*. For instance, associating a risk to a control objective implicitly provides a rationale for the existence of a control objective and is recommended to increase model comprehension. The explicit association of risks with

control objectives enables further analyses for auditing purposes (e.g., identification of risks without controls and vice versa [SP02]). Also note that *Requirement 2—System of internal controls* is addressed by the recursive association between control objective types to allow for links between internal controls. Those links enable further analyses such as which IT controls impact which business controls. Figure 3 illustrates a corresponding specification of *ControlObjective*.

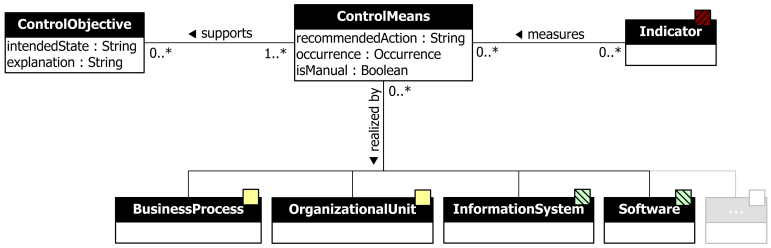


Figure 4: Conceptualization of "control means"

Control Means. Following our earlier analysis, we propose to conceptualize the meta type *ControlMeans* as an abstraction over both static and dynamic aspects of the means to achieve control. In the light of *Requirement 4—Diversity of implementation*, the conceptualization shown in Fig. 4 is aimed at providing flexibility while at the same time providing a structure for auditing purposes. We suggest to specify the recommended course of action by a natural language specification, *recommendedAction*. Such a specification could mention written policy and corresponding procedures. Further semantics is specified by *occurrence* to classify control means into preventive, detective or corrective controls according to their effect in time relative to the occurrence of a risk [GSF04, 253]. Another characteristic is captured by a functional differentiation between manual and automated control activities, *isManual*. Control means may be linked to indicators measuring the effectiveness and efficiency of a particular means by associating the meta type *ControlMeans* to the meta type *Indicator* which, for example, provides semantics to create comprehensive indicator systems [FHK09]. From the analysis in the previous sections we conclude that (1) multiple means exist that can be deployed to achieve a control objective; (2) the same means can be reused by several control objectives; (3) a certain means can pertain to several structural *and* procedural elements and thus exhibit a "multidimensional" characteristic (e.g., a written policy corresponding with a process "Authorize credit"). One approach would be to introduce dedicated concepts to represent the intricacies of control means (e.g., modeling concepts for policy and procedure). We have currently refrained from that option for two reasons: (1) The multitude of control means (e.g., [GSF04, 253ff.]) suggests the need for a high degree of flexibility with respect to representing the spectrum of relevant measures and the abstractions they refer to (cf. Req. 4); (2) by associating control means with existing concepts such as *BusinessProcess*, *OrganizationalUnit* or *InformationSystem* the semantics of many cases can be covered through additional organizational context (cf. Req. 1). For example, a control means "Segregation of duties" can be associated with a business process "Authorize credit" and with an information system "ERP system" to

implement a written policy. The current proposal, however, poses a number of notational problems, for example, how to visually identify all elements belonging to an internal control and its means. Introducing overlay symbols on notation elements is a response to this issue but relies on tool support and may, in practical applications, sacrifice clarity of the graphical notation. In the following, we will discuss further design issue with regard to our proposal.

6.2 Design issues

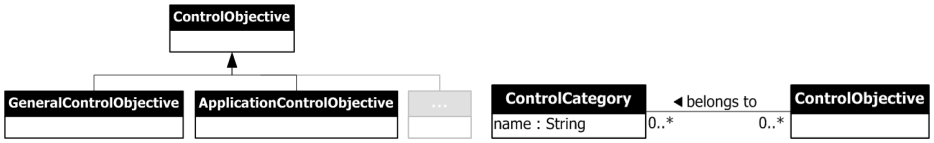
Involvement of organizational roles. A design issue relates to the different types of involvement that organizational roles—i.e., stakeholders—can have in relation to control objectives. Both, domain analysis and application scenario suggest differentiating the involvement of organizational roles into internal controls. For instance, the IT Governance Institute suggests four types of involvement in the well-known RACI charts [IT 07]: Responsible, Accountable, Consulted, and Informed. Thus, the conceptualization of the relation between roles and control objectives in Fig. 3 will probably not be sufficient for audit risk assessment purposes, as it lacks any elaborated semantics. Figure 5 illustrates two design alternatives that are feasible to represent these types of involvement: First, for each identified type of involvement a particular association between the meta-types representing the organizational role and the control objective is established (cf. Fig. 5(a)). Second, a meta-type serves as an "association class" between organizational role and control objective and allows for instantiating these four—and further—associations (cf. Fig. 5(b)). While the first alternative restricts modelers to predefined types of involvement and their min/max-cardinalities—and is thus likely to promote a more secure modeling; the second alternative provides more flexibility for modelers to add company-specific relations (e.g., "supports") without adapting the meta-model.

(a) Specification using associations (b) Specification using a meta type

Figure 5: Design alternatives for the specification of the involvement of organizational roles

Control Categories. Audit literature proposes several typifications of controls, among other, general controls, business process controls, financial controls (accounting perspective), and IT controls (IT operations perspective). In the field of IT risk management, further, possibly overlapping categories are general IT controls, pervasive IT controls, detailed IT controls, and application controls (e.g., [Inf09, 25]). When modeling a system of internal controls, it, thus, contributes to the reduction of complexity if control objectives are properly classified by their type of control. One solution to allow for representing such types would be to offer specific meta types that are specializations of the control objective, e.g., meta types *ApplicationControlObjective* and *GeneralControlObjective* (cf. Fig. 6(a)). Again, such a solution would restrict the users to predefined, disjunct types but at the same

time promote a secure modeling. On the other hand, the control category can be represented by a meta type that allows enterprises for instantiating their own categorization as well as having overlapping categories (cf. Fig. 6(b)). Since we are not aware of a widely accepted categorization of controls, we recommend to establish a flexible meta type *ControlCategory* which enables enterprises to build their own systematization.



(a) Specification using Specialization (b) Specification using a meta type

Figure 6: Design alternatives for the specification of control categories

Monitoring and auditing processes So far, we have abstracted from the procedural, dynamic aspects of internal controls (such as the regular monitoring and auditing of refund transactions, cf. Fig. 2). In principle, those processes exhibit characteristics similar to business processes: They consist of a set of activities following a control flow (e.g., sequence, concurrency and alternative) and are performed by organizational units (usually internal or external auditors). However, an initial analysis of the peculiarities of audit processes reveals an interesting difference: While business processes are performed on a regular basis, usually in high frequency each day, audit processes, in contrast, may have very different frequencies that range from an event-driven instantiation to several instantiations per month or year to a continuous (since automated) execution. Also, audit processes differ from business processes in that they are specifically designed to run "outside" of a firm's regular operations with the intention to control a particular "audit object" such as a business process, a record of transactions etc.

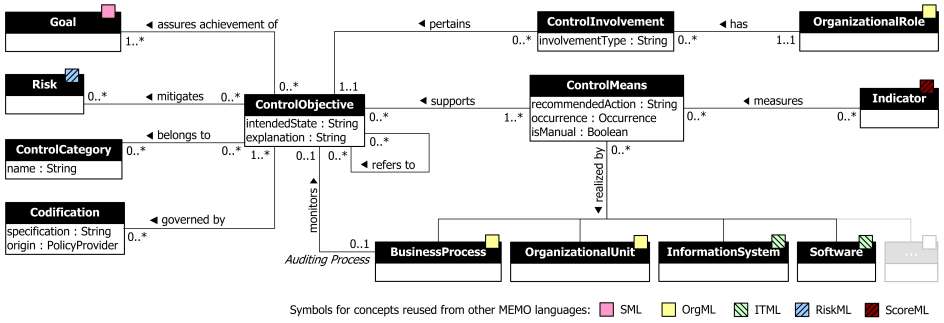


Figure 7: Specification of modeling concepts for internal controls modeling (meta model specified using the MEMO Meta Modeling Language [Fra08])

In a sense, audit processes are, therefore, associated with the specific audit object(s). However, present process modeling approaches—to our knowledge—do not provide modeling constructs to represent such qualified associations between processes (e.g., "controls",

"audits") or frequencies. Hence, we identify this as an open design issue for future research which may require further exchange with domain experts. As a workaround, we propose to utilize those business process modeling approaches for modeling auditing and monitoring processes that provide time-related events. As the MEMO business process modeling language includes differentiated concepts for temporal events, it seems feasible to reuse the *BusinessProcess* concept as is shown in Fig. 7 (see the role *Auditing Process*). The meta model consolidates the discussed design decisions and provides a foundation for future work on internal controls modeling.

7 Conclusions

This paper investigates the potentials of an enterprise modeling approach to audit risk assessment and proposes conceptualizations for modeling constructs as enhancements to enterprise modeling to support audit risk assessment. The approach is based on the assumption that enterprise models provide a substantial foundation for audit risk assessment in that they represent the organizational context (Req. 1) and support multiple perspectives (Req. 5).

Our contribution in this paper is threefold: First, we direct the discussion on supporting audit risk assessment through conceptual models to include further abstractions (i.e., goal models, role models and (IT) resource models) common to enterprise modeling—beyond business process modeling. Second, we refine and structure the technical terminology in the auditing domain by reconstructing key concepts. Third, we prepare for further research on a domain-specific modeling language for audit risk assessment by reflecting key considerations and decisions pertaining to internal controls modeling.

In this paper, we focus on language concepts—especially with regard to the internal control system, its justification, and implementation (cf. Req. 2–4)—and discuss design alternatives for corresponding modeling constructs as part of a design research project to develop a comprehensive enterprise modeling method for governance, risk, and compliance. However, developing a *method* requires further considerations besides language design. On the one hand, a method has to account for corresponding diagram types targeted at the perspectives of stakeholders involved in audit risk assessment (e.g., a dedicated internal control diagram as indicated in Fig. 2). On the other hand, a method demands for a process model that guides auditors and stakeholders in applying and interpreting the language concepts, for instance, for certain types of analyses. The effective and efficient use of such a method also presupposes the availability of a modeling tool that implements both the enterprise modeling method as well as the control-related enhancements. Such a methodical support remains on our research agenda and includes the MEMO modeling tool [GF10] (http://www.wi-inf.uni-due.de/fgfrank/memocenter-en).

References

[ABC04] P. Alencar, J. E. Boritz, and Carla Carnaghan. The relative merits of diagrammatic versues textual representations: a literature review of theoretical and empirical perspectives. Working paper, University of Waterloo, 2004.

[ABC08] P. Alencar, J. E. Boritz, and Carla Carnaghan. Business Modeling to Improve Auditor Risk Assessment: An Investigation of Alternative Representations. In *Proceedings of the 14th Annual International Symposium on Audit Research, ISAR 2008, Los Angeles, California, USA, May 30–31, 2008*, Los Angeles, CA, May 2008. American Accounting Association.

[AJKL06] Rakesh Agrawal, Christopher M. Johnson, Jerry Kiernan, and Frank Leymann. Taming Compliance with Sarbanes-Oxley Internal Controls Using Database Technology. In Ling Liu, Andreas Reuter, Kyu-Young Whang, and Jianjun Zhang, editors, *Proceedings of the 22nd International Conference on Data Engineering, ICDE 2006, 3–8 April 2006, Atlanta, GA, USA*, page 92. IEEE Computer Society, 2006.

[ALM02] T. S. Amer, R. F. Lucy, and J. Maris. The effects of system representation on the efficiency and effectiveness of control and maintenance reviews. Technical report, Northern Arizona University, Flagstaff, AZ, 2002.

[Car06] Carla Carnaghan. Business process modeling approaches in the context of process level audit risk assessment: An analysis and comparison. *Int J of Account Inf Syst*, 7(2):170–204, 2006.

[CL03] K. T. Chen and Ronald M. Lee. Knowledge-based evaluation of internal accounting control systems — a pattern recognition approach. In *Proceedings of the American Accounting Association Conference*, Honolulu, HI, 2003.

[CS02] Margaret Crawford and William Stein. Auditing Risk Management: Fine in Theory but who can do it in Practice? *International Journal of Auditing*, 6(2):119–131, 2002.

[Dam05] Marios Damianides. Sarbanes-Oxley and IT Governance: New Guidance on IT Control and Compliance. *Inf. Sys. Manage.*, 22(1):77–85, 2005.

[DCH05] Cheryl Lynn Dunn, J. Owen Cherrington, and Anita Sawyer Hollander. *Enterprise Information Systems: A Pattern-Based Approach*. McGraw-Hill Irwin, Boston, MA, 3. ed., internat. ed. edition, 2005.

[Dun06] Cheryl L. Dunn. Business Process Modeling Approaches in the Context of Process Level Audit Risk Assessment: An Analysis and Comparison : Discussion Comments. *International Journal of Accounting Information Systems*, 7(2):205–207, 2006.

[FHK09] Ulrich Frank, David Heise, and Heiko Kattenstroth. Use of a Domain Specific Modeling Language for Realizing Versatile Dashboards. In Matti Rossi et al, editor, *Proceedings of the 9th OOPSLA workshop on domain-specific modeling (DSM)*, 2009.

[Fra02] Ulrich Frank. Multi-Perspective Enterprise Modeling (MEMO): Conceptual framework and modeling languages. In *Proceedings of the 35th Annual Hawaii International Conference on System Sciences (HICSS)*, pages 72–82, Honululu, 2002.

[Fra08] Ulrich Frank. The MEMO Meta Modelling Language (MML) and Language Architecture. ICB Research Report 24, Institute for Computer Science and Business Information Systems (ICB), Duisburg-Essen University, Germany, 2008. http://www.icb.uni-due.de/fileadmin/ICB/research/research_reports/ICBReport24.pdf.

[GF10] Jens Gulden and Ulrich Frank. MEMOCenterNG. A full-featured modeling environment for organisation modeling and model-driven software development. In Pnina Soffer and Erik Proper, editors, *Proceedings of the CAiSE Forum (Short Papers and Tool Demonstrations) of the 22nd International Conference on Advanced Information Systems Engineering (CAiSE'10), 7–11, June 2010*, Lecture Notes in Business Information Processing, Berlin, Heidelberg, 2010. Springer. To appear.

[GHSW08] Guido Governatori, Jörg Hoffmann, Shazia Wasim Sadiq, and Ingo Weber. Detecting Regulatory Compliance for Business Process Models through Semantic Annotations. In Danilo Ardagna, Massimo Mecella, and Jian Yang, editors, *Business Process Management Workshops*, volume 17 of *Lecture Notes in Business Information Processing*, pages 5–17. Springer, 2008.

[GMS06] Guido Governatori, Zoran Milosevic, and Shazia Sadiq. Compliance checking between business process and business contracts. In *Proceedings of the 10th IEEE International Enterprise Distributed Object Computing Conference (EDOC'06), Hong Kong, China, Oct 16, 2006*, pages 16–20, Los Alamitos, CA, USA, October 2006. IEEE Computer Society.

[GSF04] Ulric J. Gelinas, Steve G. Sutton, and Jane Fedorowicz. *Business processes and information technology*. South-Western Thomson Learning, Mason, Ohio, 2004.

[Inf09] Information Systems Audit and Control Association. IS Standards, Guidelines and Procedures for Auditing and Control Professionals. Rolling Meadows, 2009.

[IT 07] IT Governance Institute, editor. *CobiT 4.1: Framework, Control Objectives, Management Guidelines, Maturity Models*. IT Governance Institute of the Information Systems Audit and Control Association, Rolling Meadows, 2007.

[Kir05] L. Kirchner. Cost Oriented Modelling of IT-Landscapes: Generic Language Concepts of a Domain Specific Language. In J. Desel and U. Frank, editors, *Proceedings of the Workshop on Enterprise Modelling and Information Systems Architectures (EMISA 2005)*, pages 166–179, 2005.

[KMS07] Dimitris Karagiannis, John Mylopoulos, and Margit Schwab. Business Process-Based Regulation Compliance: The Case of the Sarbanes-Oxley Act. In *Requirements Engineering*, pages 315–321. IEEE, 2007.

[Lan05] M. Lankhorst. *Enterprise Architecture at Work : Modelling, Communication and Analysis*. Springer, Berlin, 2005.

[LSG08] Ruopeng Lu, Shazia Wasim Sadiq, and Guido Governatori. Measurement of Compliance Distance in Business Processes. *Inf. Sys. Manag.*, 25(4):344–355, 2008.

[Mai00] Steven Maijoor. The Internal Control Explosion. *International Journal of Auditing*, (4):101–109, 2000.

[McC79] W. E McCarthy. An entity-relationship view of accounting models. *The Accounting Review*, 54(4):667–686, 1979.

[McC82] W. E McCarthy. The REA accounting model: A generalized framework for accounting systems in a shared data environment. *The Accounting Review*, 57(3):554–578, 1982.

[Moe08] Robert R. Moeller. *Sarbanes-Oxley Internal Controls : Effective Auditing with AS5, CobiT and ITIL*. John Wiley & Sons, Hoboken, NJ, 2008.

[NS07] Kioumars Namiri and Nenad Stojanovic. Applying Semantics to Sarbanes Oxley Internal Controls Compliance. In Rainer Koschke, Otthein Herzog, Karl-Heinz Rödiger, and Marc Ronthaler, editors, *GI Jahrestagung*, volume 109 of *Lecture Notes in Informatics*, pages 222–226. GI, 2007.

[PP97] Jens Pitthan and Mathias Philipp. Einsatz von Petri-Netzen für die Aufnahme, Dokumentation und Analyse Interner Kontrollsysteme im Rahmen der Jahresabschlußprüfung. In W. Stucky and U. Winand, editors, *Petri-Netze zur Modellierung verteilter DV-Systeme – Erfahrungen im Rahmen des DFG-Schwerpunktprogramms "Verteilte DV-Systeme in der Betriebswirtschaft"*, number 350, pages 87–104. Institut für Angewandte Informatik und Formale Beschreibungssprachen (AIFB), Universität Karlsruhe (TH), Karlsruhe, Germany, March 1997.

[RBGR06] P. Rikhardsson, P. Best, P. Green, and M. Rosemann. Business Process Risk Management, Compliance, and Internal Control: A Research Agenda. Technical report, Department of Business Studies, Management Accounting Research Group, Aarhus School of Business, Aarhus, Denmark, 2006.

[Sch92] A.-W. Scheer. *Architecture of Integrated Information Systems : Foundations of Enterprise Modelling*. Springer, Berlin, 1992.

[Sch00] A.-W. Scheer. *ARIS : Business Process Modeling*. Springer, Berlin, Heidelberg, 3 edition, 2000.

[SGN07] Shazia Wasim Sadiq, Guido Governatori, and Kioumars Namiri. Modeling Control Objectives for Business Process Compliance. In Gustavo Alonso, Peter Dadam, and Michael Rosemann, editors, *BPM 2007*, volume 4714 of *Lecture Notes in Computer Science*, pages 149–164, Berlin, 2007. Springer.

[SHF10] Stefan Strecker, David Heise, and Ulrich Frank. RiskM: A multi-perspective modeling method for IT risk assessment. *Information Systems Frontiers. Accepted for publication in the Special Issue on Governance, Risk and Compliance Applications in Information Systems*, 2010.

[SLKP07] Amadou Sienou, Elyes Lamine, Achim Karduck, and Hervé Pingaud. Conceptual Model of Risk: Towards a Risk Modelling Language. In Mathias Weske, Mohand-Said Hacid, and Claude Godart, editors, *WISE Workshops*, volume 4832 of *Lecture Notes in Computer Science*, pages 118–129. Springer, 2007.

[SP02] L. F. Spira and M. Page. Risk Management — The reinvention of internal control and the changing role of internal audit. *Accounting, Auditing & Accountability Journal*, 16(4):640–661, 2002.

[The92] The Committee of Sponsoring Organizations of the Treadway Commission. Internal Control — Integrated Framework, September 1992.

[The04] The Committee of Sponsoring Organizations of the Treadway Commission. Enterprise Risk Management – Integrated Framework (Executive Summary), September 2004.

[The09] The Committee of Sponsoring Organizations of the Treadway Commission. Guidance on Monitoring Internal Control Systems: Introduction. http://www.coso.org, 2009.

[The10] The Committee of Sponsoring Organizations of the Treadway Commission. What is internal control? http://www.coso.org/resources.htm, September 2010.

[zMR05] M. zur Muehlen and M. Rosemann. Integrating Risks in Business Process Models. In *Proceedings of the 16th Australasian Conference on Information Systems (ACIS 2005)*, pages 62–72, 2005.