Stefan Strecker, David Heise, Ulrich Frank

Prolegomena of a modelling method in support of audit risk assessment

Outline of a domain-specific modelling language for internal controls and internal control systems

Internal controls constitute a key concept in the auditing domain. In the audit risk assessment process, auditors evaluate a firm's internal control system to provide reasonable assurance regarding the achievement of the entity's objectives. The present work reflects upon the design of a domain-specific modelling language for internal controls modelling. It investigates the potentials of an enterprise modelling approach to audit risk assessment, reconstructs technical terminology in the auditing domain, and discusses design decisions and design alternatives by means of tentative language specifications.

1 Introduction

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 (Ramos 2004; Dunn et al. 2005, p. 433). 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 (Sutton and Hampton 2003). As relevant risks pervade the enterprise from operations to corporate strategising (Westerman and Hunter 2007), it needs to be questioned '[w]hy limit the analysis to the business process level?' (Dunn 2006, p. 207)—when legal regulations and auditing standards prescribe assessing risks at all relevant levels of the organisation (COSO 1992; ISACA 2009). Audit risk assessment thus pertains to any risk of not achieving business objectives; not only risks related to financial reporting (Crawford and Stein 2002). Hence, auditing standards 'emphasize the importance of auditors gaining a broader understanding of an organization' (Carnaghan 2006, p. 171). Hence, auditors are confronted with the remarkable complexity of present day enterprises (Rikhardsson et al. 2006). They are required to understand a firm's business, its risks and controls in place to treat risk exposure at all relevant organisational levels which implies an understanding of entity objectives, business processes, organisational resources, structures, roles, and responsibilities (Elder et al. 2010). Auditors also have to deal with the complexity of internal control systems themselves: Controls occur for multiple organisational 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 (Maijoor 2000). 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 (Spira and Page 2002). In this respect, the complexity challenge is intensified by different technical languages, differing mindsets, and resulting barriers to communicate—hampering in particular the cooperation between auditor and auditee.

The auditing literature recognises the potentials of supporting audit risk assessment through conceptual models (e.g., Bradford et al. 2007), in particular business process models in the context of process-level audit risk assessment (e.g., ISACA 2009, p. 132). It is, however, acknowledged that present generic approaches to business process modelling do not provide adequate modelling constructs required for representing internal control systems with regard to effectively and efficiently supporting auditors when performing audit risk assessment (Carnaghan 2006). In particular, it is criticised that present approaches focus on the business process level and do not provide support for appropriately representing further relevant organisational context such as business objectives, organisational resources, roles and their responsibilities (Dunn 2006). Such modelling concepts are, however, common to enterprise modelling approaches such as ARIS (Scheer 1992), SOM (Ferstl and Sinz 1998) and MEMO (Frank 1994, 2008) which supplement business process models with further abstractions of the enterprise and its organisational action systems (i.e., conceptual models of organisational goals and strategies, structures, roles and resources). While current enterprise modelling approaches thus provide support for necessary organisational context, they do not, to our best knowledge, entail elaborate domain-specific modelling concepts for representing internal controls and internal control systems.

The present work reflects upon the design of a domain-specific modelling language for internal controls modelling. It investigates the potentials of an enterprise modelling approach to audit risk assessment, reconstructs technical terminology in the auditing domain, and discusses design decisions and design alternatives by means of tentative language specifications. This work is part of an ongoing design research project whose overall purpose is to effectively and efficiently support auditors when performing audit risk assessment. More specifically, the project is aimed at developing a comprehensive modelling method supporting auditors in understanding a firm's business, its operations and processes, associated risks and internal controls when assessing the risk of material misstatement Strecker et al. 2010. Given that the auditors' understanding is educed in group processes (Damianides 2005, p. 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. In particular, the method comprises domain-specific modelling languages in support of dedicated analyses. Each language provides modelling concepts that foster the reduction of complexity by providing appropriate abstractions and a corresponding graphical notation; that allow for structuring the complex subject in a purposeful way. Hence, they promote transparency of internal control matters, specifically by visually representing internal controls as part of the organisational action systems, and by improving traceability of the controls in place to treat risk exposure. Thus, the language application viz. type level models provide an elaborate medium to fostering and facilitating communication among stakeholders involved in audit risk assessment—with a dedicated focus on auditor and auditee interaction. Moreover, they serve as a conceptual foundation for developing corresponding software tools for modelling, analysis, and decision-making.

The next section reviews related work. Section 3 reconstructs technical terminology in the auditing domain. It also refines the design goals and reasons about requirements a method aimed at supporting audit risk assessment should satisfy. The general prospects of an enterprise modelling approach to audit risk assessment are investigated in Section 4. In Section 5, we reflect upon the design of domain-specific modelling constructs and discuss key design issues. Section 6 summarises findings and discusses paths for further research.

2 Related work

Since McCarthy (1979, 1982)'s work on the REA (resources, events, agents) model, auditing and

accounting information systems literature recognises the use of conceptual models of the enterprise for supporting accountants and auditors in understanding a firm's business (e.g., Dunn et al. 2005; Gelinas et al. 2004). Behaviorist research indicates that graphical representations of the enterprise advance the understanding of auditors over text-based documentation (Alencar et al. 2004; Amer et al. 2002; Dunn and Gerad 2001). Studies on the actual use of graphical representations in audit risk assessment processes support anecdotal evidence that system flowcharts (cf. Fig. 1 on the next page) and data flow diagrams are still the predominant means of graphical representation used in audit reviews (Gelinas et al. 2004, p. 24). A recent study shows, however, that business process modelling approaches such as the Business Process Model and Notation (BPMN) or the extended Event-driven Process Chain (EPC) approaches are gaining increasing acceptance in the auditing domain (Alencar et al. 2008).

Carnaghan (2006) reviews different business process modelling notations with regard to their support for process-level audit risk assessment. She concludes that present approaches do not allow for adequately expressing the semantics of internal controls and, consequently, further modelling constructs are required. 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' (Dunn 2006, p. 207). Their assessment, however, ignores contributions from the conceptual modelling community to the auditing domain.

Petri nets have for long been discussed as a means to document business processes and corresponding internal controls aimed at algorithmic verification of compliance (Chen and Lee 2003; Pitthan and Philipp 1997). Sadiq et al. (2007) interpret internal controls in terms of rules and target rule-based compliance checking based on automated reasoning (for related approaches, see e.g., Governatori et al. 2006, 2008; Lu et al. 2009). Another rule-based approach to modelling internal control systems is described by Bailey, Jr. Et al. (2000) based on a PROLOG implementation. Conceptualising internal controls as formal rules may complement domain-specific modelling constructs for internal controls modelling to enable compliance checking based on graphical models of the internal control system.

The work by Karagiannis et al. (2007) is among the first to consider domain-specific modelling concepts dedicated to internal controls modelling. Three SOX-related domain-specific modelling concepts, Control, Risk, and Account, are mentioned as an extension to an enterprise modelling approach and a corresponding modelling tool. Language concepts are specified as a metamodel (see also Karagiannis 2008, p. 1164) and related to further concepts for risk management such as Event and Action. Interpretation of the semantics of modelling concepts is, however, partly left to the language user, since the metamodel does not show attributes and the accompanying documentation remains silent on further details. Moreover, important aspects of the design of a domain-specific modelling language are only briefly discussed, for instance, a notation and corresponding diagram types for representing internal control systems. In a series of related papers, Namiri and Stojanovic (2007a,b) identify additional domain concepts (e.g., ControlObjective, RiskAssessment, Authority), and visualise conceptual relationships in a UML class diagram notation (Namiri and Stojanovic 2007b, p. 63). Their 'domain model' structures the technical terminology in the auditing domain with the intention to 'formulate logical statements representing the controls constraining the behavior of a Business Process' (Namiri and Stojanovic 2007b, p. 62). However, the domain model does not specify syntax and semantics of a domain-specific modelling language. Though it informs the domain analysis in the next section.

3 Domain analysis

Designing domain-specific modelling concepts presupposes reconstructing key terms and their

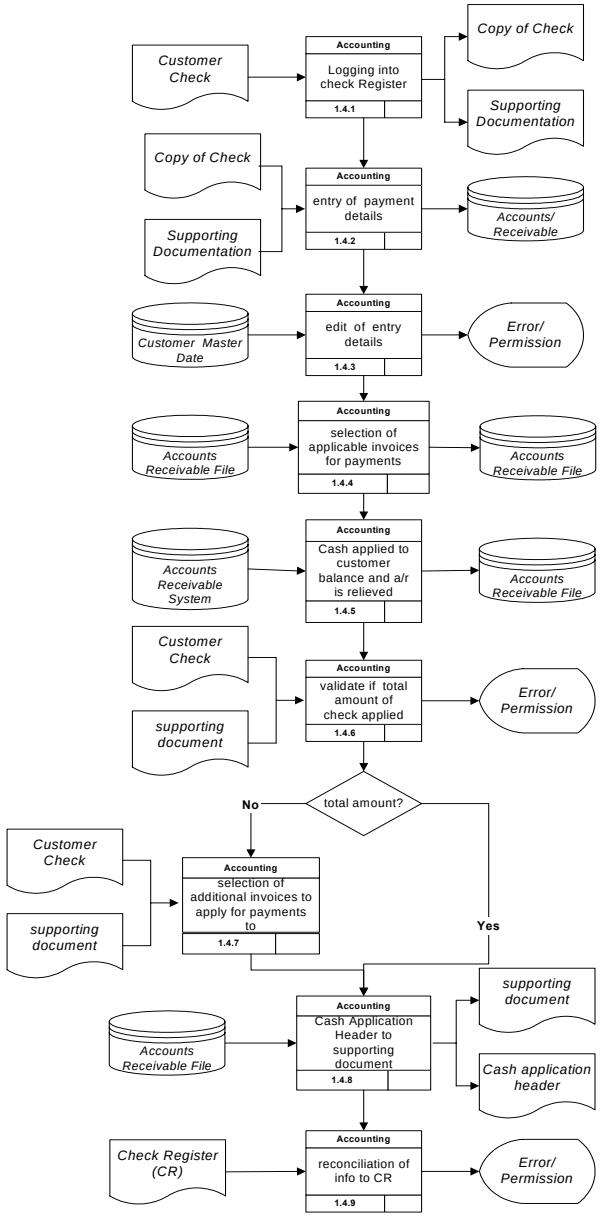
Process Flow & Controls Map	Description
	1.4.1 The checks are forwarded to the Accounting Supervisor who logs them in a Check Register. The information recorded includes date of check, check number, check amount, customer name/number, and invoices that payment relates to. The Accounting Supervisor makes copies of the checks and sends the check copies along with the invoice hard copy supporting documentation to the Cash Application Department. 1.4.2 A representative of the Cash Application Department (representative) enters the customer number into the Cash Application screen within the Accounts Receivable system. The system validates the customer number against the Customer Master (Standing Data) file within the system. 1.4.3 If the system does not find the number, an error message is displayed indicating the number is invalid. The representative has the option of entering the customer last name and first name into a search screen to locate the customer number. If the system locates the customer master record for the customer number entered, a list of open invoices is generated on to the screen. 1.4.4 The next screen is for the first invoice number selected to apply payment to. 1.4.5 The representative is prompted to enter the amount of payment being applied to the invoice on a field at the top of the screen. The amount will typically match the total invoice amount (listed on the bottom of the screen), but there are times that only partial payment is applied to a particular invoice. 1.4.6 The invoice amount entered must be numeric and cannot be for an amount greater than the amount left to apply from the payment. The representative scrolls through each invoice and applies cash to each applicable one. The system keeps a running total of the total amount of payment (per the check) and the amount left to be applied. 1.4.7 The representative cannot close out of the Cash Application screen without applying the total check amount to the open invoices. 1.4.8 The representative is responsible for printing out the Cash Application Header screen showing the high-level details of the cash application payment including check number, check amount, and check date. The representative staples the Cash Application Header screen printout to the check copy and supporting documentation. This information is forwarded back to the Accounting Supervisor at the end of the day. 1.4.9 The Accounting Supervisor reconciles the documentation back to the Check Register to ensure all checks were applied.

Figure 1: Illustration of how business processes and internal controls are commonly documented in auditing practice: 'Example of a Level 2 Flowchart: Cash Application Sub-process Showing Transactions and Controls' (Pricewaterhouse-Coopers 2004, p. 104).

semantics in the targeted domain (Ortner 2008). Reconstruction of a technical terminology is an iterative process involving more than the identification of candidate (meta) concepts, their attributes and relations. Instead it requires, for instance, the identification and resolution of terminological ambiguity and truncation, which may imply the introduction of additional abstractions. That in turn may require the shaping of their semantics. This implies the (re-)interpretation of observed terms and concepts and leads to design abstractions appropriate for specific analyses and applications. The method engineering approach underlying the present work is therefore driven by analyzing application scenarios describing, among others, model-based analyses, and by interpreting pertinent literature in the field under consideration (Frank 2010). This section summarises key findings from the conceptual reconstruction of the technical terminology in the auditing domain.

3.1 Terminological analysis

In auditing literature and practice, 'control', 'internal control', and 'internal control system' are commonly used terms (Moeller 2008). Despite their proliferation, a lack of precise definition and understanding of even these key domain concepts has repeatedly been criticised (Maijoor 2000). The term 'control' is in fact subject to a considerable diversity of disciplines, for example, 'management control, organisational control, internal controls, operational control and financial control, which all seem to revolve around the same concept' (Rikhardsson et al. 2006). The auditing perspective on *internal* control is decisively influenced by the Committee of Sponsoring Organizations of the Treadway Commission (COSO) (COSO 1992, 2004) and subsequent auditing standards such as the Public Company Accounting Oversight Board (PCAOB) Auditing Standard No. 5 (for a discussion see Rikhardsson et al. 2006 and Maijoor 2000): '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 organisation. [...]' (COSO 2010; adapted from COSO 1992).

While this very broad conceptualisation 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 (i.e., business processes, auditing and monitoring processes) and structural aspects (e.g., policies, organisational structures, organisational roles). 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' (COSO 2004). The COSO framework, in fact, breaks down internal control to five interrelated components: Control Environment, Risk Assessment, Control Activities, Information and Communication as well as Monitoring (Gelinas and Dull 2010, pp. 224–225).

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. 2. It is mainly based on an analysis of the reviewed prior work,

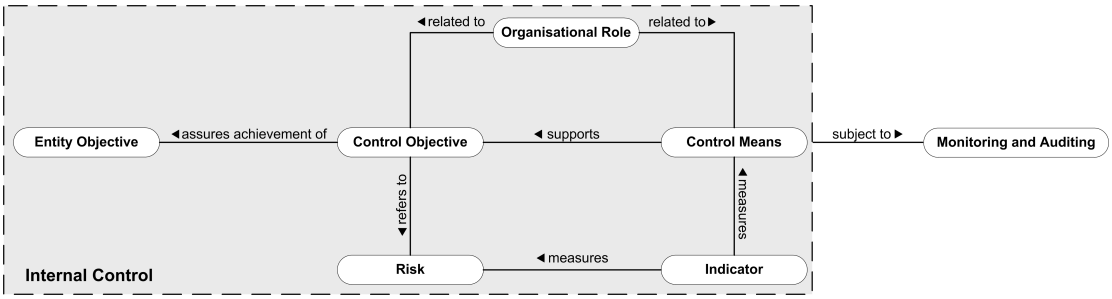


Figure 2: Initial reconstruction of essential domain terminology: Domain-specific concepts visualised as a semantic net.

the mentioned COSO documentation, four textbooks (Dunn et al. 2005; Elder et al. 2010; Gelinas and Dull 2010; Gelinas et al. 2004) as well as anonymised audit documents received from a Big Four auditor.

A key domain concept is *control objective*, sometimes also denoted as control goal (Gelinas et al. 2004, p. 249). It represents a desired state of an enterprise ('Prevent unauthorised refunds') with respect to achieving an *entity objective* ('Minimise 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 organisational structures as concrete measures or means of control implemented to ensure effectiveness of a control (Elder et al. 2010). An important means to prevent fraud is 'segregation of duties' (Gelinas and Dull 2010, p. 255). Segregation of duties is aimed at preventing unauthorised transactions in a given organisational context (e.g., a refund returned goods process). 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 organisational structures and dynamic means of control such as activities and procedures. Alternative denominators to the control means concept could have been 'control activity' (IT Governance Institute 2007) and 'control plan' (Gelinas et al. 2004, p. 249). Both, however, entail a significant risk of misinterpretation: The term 'activity' raises associations with dynamic abstractions neglecting static aspects while the term 'plan' emphasises a perspective different from the intended means-end association. Examples for general control means given in COSO publications include the authorisation 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 conceptualisation: 'Responsible', 'Accountable', 'Consulted', 'Informed') are defined typically for more than one *organisational role* ('executive', 'business process owner', etc.) with respect to a control objective. It is important to 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 (COSO 2009).

Figure 3 on the next page illustrates further descriptives of internal controls. It shows a sample control matrix as used in auditing practice (Gelinas and Dull 2010, p. 227). A (process and) control matrix matches control objectives with relevant control means grouped by business processes (Gelinas and Dull 2010, p. 649).

Sub-Process	Control Objective	Description and Frequency of Control Activity	Financial Statement Area (1)	Information Processing Objectives (C,A,V, R) (2)	Assertions (CO, EO, RO, VA, PD) – (3)	P or D (4)	A or M (5)
Invoicing	Sales invoices are accurate.	The billing system receives shipped items from the shipping system and compares, line by line, the shipped items to the original order, making changes to the original order to reflect actual quantities shipped. (Multiple times a day)	Sales	C, A, V	CO, EO, VA	P	A
Invoicing	A sales invoice is generated for every shipment or work order.	Before an invoice is processed, shipment information is matched to customer-order information to ensure the information's accuracy and validity. (Multiple times a day)	Sales	A,V	A,C,E/O	P	A
G/L Posting	Sales are recorded in the proper period.	Management monitors sales and margins to ensure that they are aligned with expectations. (Monthly)	Sales	C, A, V	C,E/O	D	M
G/L Posting	Sales are recorded in the proper period. Postings that are made to cost of sales and/or inventory in the general ledger are appropriate.	The finance department reconciles sales in the general ledger with shipments on a weekly basis and follows up any reconciling items. This reconciliation is signed and filed. (Weekly)	Sales	C, A, V	C,E/O	D	M

1. Financial-statement area (F/S area)
2. Completeness (C), accuracy (A), validity (V), and restricted access (R)
3. Completeness (CO); existence or occurrence (EO); rights and obligations (RO); valuation or allocation (VA); and presentation and disclosure (PD)
4. Preventive (P) or detective (D) control
5. Automated (A) or manual (M) control

Figure 3: Illustration of how internal controls are commonly documented as part of audit evidence: 'Sample Control Matrix' (PricewaterhouseCoopers 2004, p. 105) showing further descriptives of internal controls (e.g., operation mode differentiation between automated and manual control).

3.2 Requirements analysis

The principal design goals stated in the introductory section—reducing complexity, fostering communication and collaboration, and improving transparency—are refined to establish five domain-specific requirements a domain-specific modelling language aimed at supporting internal controls modelling should satisfy. The requirements analysis is informed by discussions with auditors at a Big Four auditing firm and is based on the prior terminological analysis including the reviewed body of literature. Both the requirements and the identified domain concepts guide the following reflection on the design of a domain-specific modelling language (DSML) for internal controls modelling.

Requirement 1—Organisational context: A DSML should link internal controls to the surrounding organisational action system composed of all organisational entities relevant to audit risk assessment. This organisational context is provided by (at least) entity objectives, business processes, business risks, performance measures, organisational resources, structures, roles and their responsibilities (Carnaghan 2006, p. 177).

Rationale. The organisational context in which an internal control is designed to be used is of particular importance to its accurate interpretation (Spira and Page 2002; Sutton and Hampton 2003), especially since legal regulations and auditing standards prescribe assessing risks at all relevant levels of the organisation (COSO 1992; ISACA 2009). Providing explicit and qualified relationships between controls and organisational context as part of a DSML is seen as both a contribution to reducing the complexity inherent to internal control systems, and to improving transparency of internal control matters.

Requirement 2—Multiplicity of control means: A DSML should account for the multiplicity of actual means to achieve control objectives and of the resulting variety of internal control implementation.

Rationale. A wide spectrum of ways to achieve control objectives is discussed employing a multitude of different organisational measures including policies and procedures, manual and automated controls (Elder et al. 2010; Gelinas and Dull 2010). Providing appropriate abstractions of control means as part of a DSML is seen as a contribution to improving transparency of internal control matters, and to reducing the complexity of internal control systems.

Requirement 3—System of internal controls: A DSML should account for relationships among internal controls on different organisational levels, from IT operations to business processes to value chains to the organisation as whole.

Rationale. PCAOB Auditing Standard No. 5 and other regulations assume relationships between internal controls as expressed, for instance, by a control hierarchy (Gelinas and Dull 2010, p. 241). Relations between internal controls need not, however, be strictly subordinate. Rather, controls relate to each other in often unspecified ways as, for example, exemplified by common typifications of controls (Dunn et al. 2005, p. 455). Providing explicit and qualified relationships among controls as part of a DSML is seen as a contribution to reducing the complexity of internal control systems, and to improving transparency of internal control matters.

Requirement 4—Justification and assumptions: A DSML should provide means for justifying the existence and importance of an internal control and for revealing assumptions underlying internal control justification.

Rationale. It has repeatedly been suggested to foster communication and collaboration on internal control matters by annotating assertions underlying the control specification and its intended usage (Carnaghan 2006, p. 177). It is assumed that by providing a traceable rationale of an internal control, accurate interpretation by auditors is fostered and communication barriers are lowered.

Requirement 5—Support for multiple perspectives: A DSML 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.

Rationale. Audit risk assessment as a group process involves stakeholders with different professional backgrounds and responsibilities as well as specific sentiments about internal controls and their effects (Spira and Page 2002). To foster communication among these stakeholders, a DSML in support of audit risk assessment needs to take the perspectives of stakeholders with different backgrounds—from senior management to IT operations—into account.

4 Analysis of the potentials of an enterprise modelling approach

This section illustrates the prospects of supporting audit risk assessment with domain-specific modelling concepts integrated with an enterprise modelling approach. The analysis is based on two presuppositions: First, it is assumed that the enterprise modelling method is based on a language architecture that allows for reuse of existing modelling concepts (for an example, see Frank 2008). Second, the following scenario presupposes that the enterprise modelling method provides language concepts for representing control flows, goals, roles, and organisational structures as is the case, for instance, with ARIS (Scheer 1992, 2000) and MEMO (Frank 1994, 2002)—thereby providing concepts to represent the organisational context required for internal controls. The MEMO approach has been chosen to illustrate the application scenario in Fig. 4, because it fulfills both assumptions and integrates further concepts essential to audit risk assessment, in particular risk (Strecker et al. 2010), performance measures (Frank et al. 2009) and IT resources (Kirchner 2005). It is important to note that the shown diagram is not intended to predetermine a notation or to preconceptualise language concepts. 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 refunding returned goods process drawn on by Carnaghan (2006, p. 200). The original case study describes a 'refund returned goods' process of a food manufacturer incorporating four internal controls: (1) 'The sales account manager must authorise returns by completing a "return merchandise authorisation" (RMA) paper form that is sent to customer service'; (2) 'The information system restricts the ability to create, change, or delete sales order return and credit requests to authorised personnel'; (3) 'Credit notes must be approved by the A/R manager before being applied to a customer account'; and (4) 'The system only allows A/R personnel to enter credit/debit memos or receivables write-offs'. The scenario in Fig. 4 reconstructs Carnaghan (2006)'s case study using the MEMO enterprise modelling approach: It 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 organisational structure (including organisational roles and committees; top right) and a model of IT resources used in the process (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 'Authorise credit') or by shared concepts (e.g., the organisational role 'A/R manager' in both the process 'Authorise credit' and in the organisational structure model).

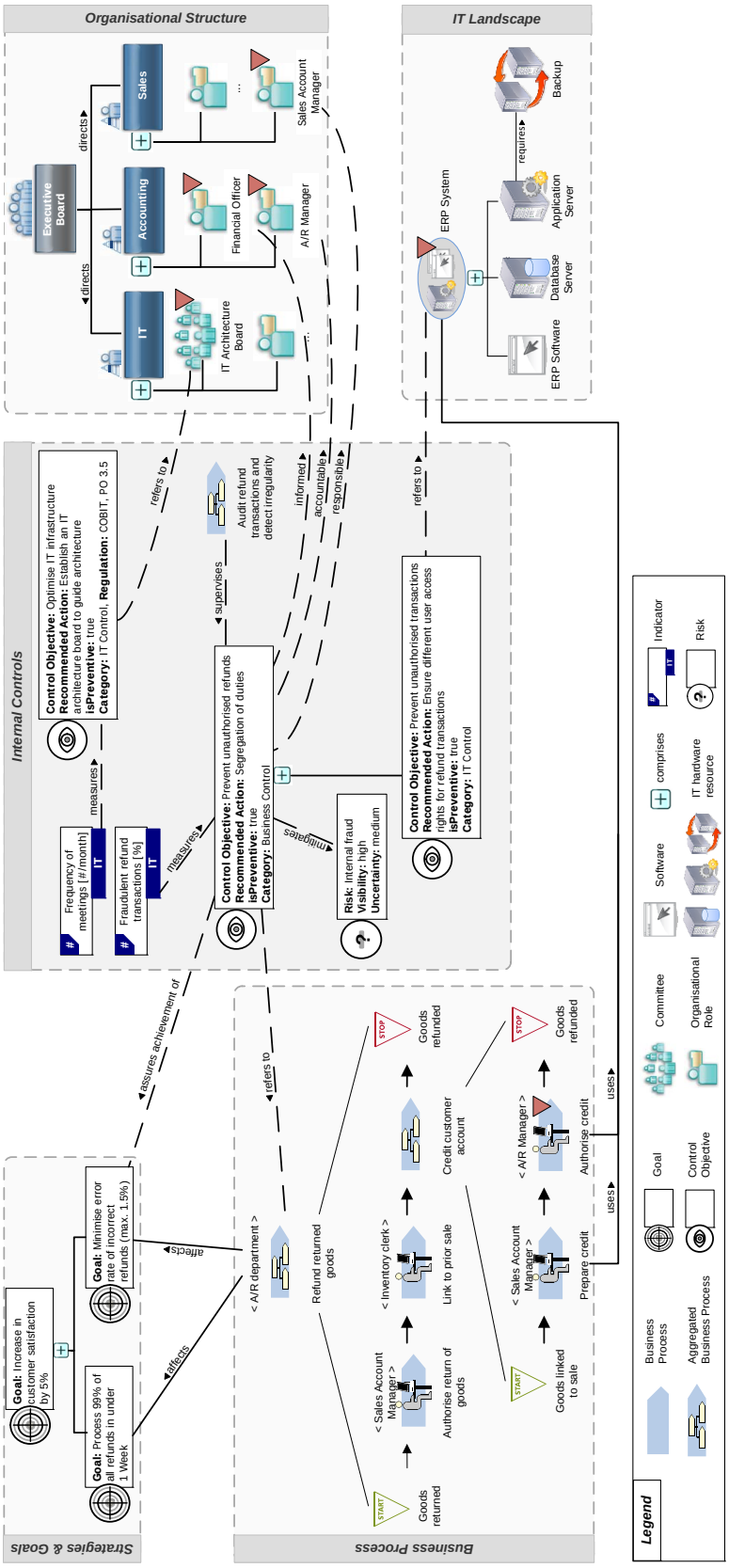


Figure 4: Illustration of an enterprise modelling approach to internal controls modelling

Provided such an infrastructure exists, internal controls modelling can be supported by extensions to existing concepts and by introduction of additional abstractions. The latter is illustrated first. The scenario shown in Fig. 4 assumes that some constituent concepts of internal controls are represented by *additional* modelling concepts. In particular, the control objective concept represents such an addition. The control objective 'Prevent unauthorised 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 unauthorised 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 modelling 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 Fig. 4, for instance, the process 'Authorise credit' is enriched with an overlay, as the process realises a significant part of the segregation of duties. Similarly, overlays are attached to the information system symbol 'ERP system' in the IT landscape model and some of the organisational units in the structure model, since these elements all relate to the internal control(s).

Figure 4 also demonstrates how the control objectives can be associated with concepts that represent the organisational 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 'Minimise error rate of incorrect refunds' in the goal model). Second, control objectives can be linked to static and dynamic abstractions representing means of control (cf. Req. 2). For example, the above mentioned control objective refers to the business process 'Refund returned goods', whereas the actual realisation 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 realises the segregation at the information system level by authorisation and system access policies. Linking the two control objectives also demonstrates how associations between controls aid in visualising internal control systems (cf. Req. 3). Associating a control objective with a corresponding risk ('Internal fraud') provides an implicitly rationale for the existence of a control objective (cf. Req. 4) possibly indicated by a performance measure ('Fraudulent refund transactions in %') . Finally, the integration with an organisational structure model emphasises different types of involvement of organisational roles as a support for multiple perspectives (cf. Req. 5). 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 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. 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 what controls exist in an enterprise, such integrated models support further analyses. On the one hand, they allow for analysing controls in respect to the organisational context they affect. For instance, in Fig. 4, 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 organisational concepts with regard to whether they are affected by controls. Especially in organisational settings that experience rapid changes such an analysis can assist in preventing failure to comply with regulations. In Fig. 4, for instance, an analysis of the committee 'IT architecture board' reveals a relationship to a control objective, so that eliminating this organisational unit from the model (e.g., as a result of a reorganisation project) raises an exception and notifies stakeholders of a likely compliance violation.

We conclude that the outlined enterprise modelling approach promises a number of advantages over textual representations, simple conceptual models or even present business process modelling approaches:

1. As a general prospect of enterprise modelling, the purposeful abstractions of the action system visualised by a descriptive graphical notation promise to reduce the complexity in analyzing a company's internal controls and, thus, announce support for internal and external auditors. The syntax and semantics of a domain-specific modelling language for internal controls modelling fosters the integrity of type level models and thus the integrity of model-based analyses for audit risk assessment purposes.
2. The proposed reuse of existing modelling concepts increases the productivity of both language design and language application. Language designers benefit from mature modelling 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 modelling 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 conceptualisation 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. The feedback received from practicing auditors on the shown application scenario indicates at least partial confirmation of this working hypothesis (as does Cendrowski et al. 2007, p. 208).

5 Considerations on language design

Based on the corroborative assessment of the potentials of an enterprise modelling approach to audit risk assessment, this section outlines general considerations toward enhancing enterprise modelling approaches with domain-specific modelling concepts for audit risk assessment, and discusses essential decisions related to the design of these modelling constructs. In this section, we present preliminary specifications of modelling constructs as metamodel excerpts. These specifications are intended as a working draft for the

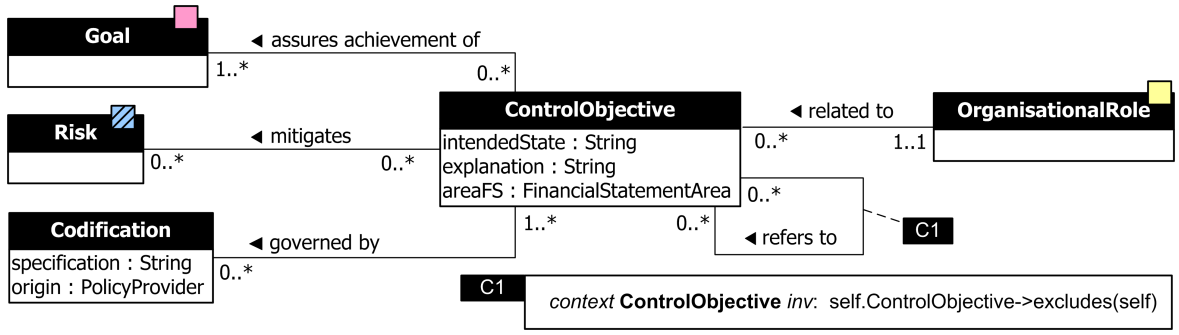


Figure 5: Tentative language design: Conceptualisation of 'control objective'

following discourse and as a foundation for discussions with and discursive evaluation by peers and domain experts.

5.1 Metamodelling foundation

The MEMO Meta Modelling Language (MEMO MML) and the corresponding language architecture (Frank 2008) serve as metamodelling foundation for the following considerations on a language design. Metamodels are specified using the MEMO MML defined at the meta-meta or M_3 level. Using MEMO MML for defining language concepts (metatypes) at the meta level (M_2) leads to integrated models at type level (M_1), e.g., an organisation structure model integrated with a business process model, a model of an IT landscape, and a model of internal controls. It also fosters reuse of existing language concepts shared among domain-specific modelling languages at the meta level (e.g., *OrganisationalUnit).* The reuse of modelling concepts from existing modelling languages in the MEMO language family is visualised by a colored rectangle attached to the metatype header indicating the concept's origin (cf. color legend in Fig. 8).

The application of language concepts specified at meta level (M_2) results in models at type level (M_1) representing particular types of items under consideration (e.g., business process types, resource types etc.). An instantiation of, for example, the metatype *ControlMeans* is a type, i.e., an abstraction over all corresponding instances in the real-world (at the instance or M_0 level). Hence, it abstracts from concrete instances such as a concrete control activity performed by a certain representative at a certain date and time. Instead, the modelling concepts constitute abstractions over corresponding instance populations.

5.2 Devising an infrastructure for internal controls modelling

The initial design decision with respect to the targeted domain pertains to the specification of language concepts (metatypes) specifying an internal control type. Following the results of the terminological analysis (cf. Sect. 3.1), it appears justified to represent an internal control by its control objective and by the means of achieving the control objective. Hence, two dedicated metatypes, *ControlObjective* and *ControlMeans*, are introduced (a similar kernel is proposed by Karagiannis 2008). To represent the semantics of internal controls, further refinements are, however, necessary and detailed below. The rationale of introducing those two metatypes is to enable dedicated audit analyses based on respective conceptual models of control objectives and control means.

ControlObjective

The *ControlObjective* concept serves to describe the intentions of an internal control. The present language specification conceptualises control objective as a dedicated language concept, the *ControlObjective* metatype (cf. Fig. 5), to allow for

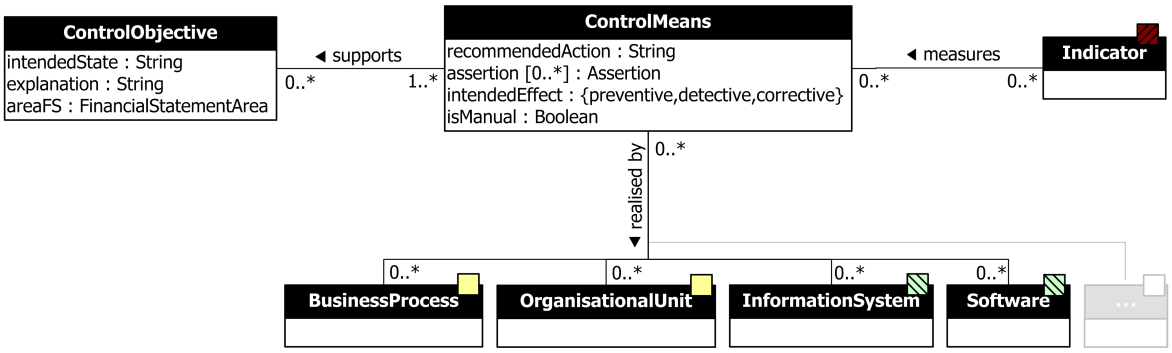


Figure 6: Tentative language design: Conceptualisation of 'control means'

modeling its relations to entity objectives *(Goal)*, risks *(Risk)* and organisational roles *(OrganisationalRole)* representing organisational context important to proper control interpretation (Req. 1). The recursive *RefersTo* association between control objective types allows to represent the internal control system as a hierarchy or net of controls (Req. 3). It enables further analyses such as which IT controls impact which business controls.

The metatype *Codification* specifies a legal regulation the control objective is governed by and its originating policy provider. 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., PCAOB Auditing Standard No. 5) as a contribution to justifying the existence and importance of an internal control (Req. 4). Associating a risk type to a control objective type also adds to a rationale for the existence of a control objective. Moreover, the explicit association of risks with control objectives enables further analyses for auditing purposes, for instance, identifying risks without controls and vice versa (Spira and Page 2002).

The *ControlObjective* modelling concept is further described by a natural language description of the desired state of control by the attribute *intendedState* ('Sales invoices are accurate', 'Prevent unauthorised refunds') and by an explanation of the intended state, *explanation* ('The billing system receives shipping items from the shipping system [...]'). In certain cases it may be feasible to rephrase the natural language specification as a formal rule to support automated reasoning on internal controls (e.g., as an additional attribute to *ControlObjective)*. Annotating the financial statement area, *areaFS*, links a control objective to financial reporting.

By associating a control objective with known visual representations of business objectives, business risks, and organisational roles, the present language design supports taking on different perspectives on internal control matters (Req. 5) where a perspective is conceptualised as a specific cognitive predisposition in the context of the MEMO method (Frank 1994, p. 164).

Control Means

The *ControlMeans* language concept serves to describe the static aspects of a means to achieve reasonable assurance. It is detailed by the recommended course of action provided in a natural language specification, *recommendedAction*. Such a specification could mention written policy and corresponding procedures ('The Accounting Supervisor makes copies of the checks and sends the check copies along with the invoice hard copy supporting documentation to the Cash Application Department'). The current conceptualisation (cf. Fig. 6) is aimed at providing flexibility while, at the same time, maintaining a structure for auditing purposes. The domain analysis

(a) Specification using associations

(b) Specification using a metatype

Figure 7: Design alternatives for specification of the involvement of organisational roles.

indicates 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 'Authorise credit'). One design approach could be to introduce dedicated concepts to represent the intricacies of control means (e.g., modelling concepts for policy and procedure). We have currently refrained from that option for two reasons: First, the multitude of control means (e.g., Gelinas et al. 2004, pp. 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. 2). Second, by associating a control means with modelling concepts such as *BusinessProcess*, *OrganisationalUnit* or *InformationSystem*, the semantics of many control activities can be described in terms of additional organisational context. For instance, a control means 'Segregation of duties' can be associated with a business process 'Authorise credit' and with an information system 'ERP system' to further describe its semantics beyond mentioning a written policy. The current proposal, however, poses a number of notational problems, for example, how to visually identify all elements constituting an internal control (and thus 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. Further semantics is specified by *assertion* (Carnaghan 2006, p. 177) and *intendedEffect* to classify control means into preventive, detective or corrective controls according to their effect in time relative to the occurrence of a risk (Gelinas et al. 2004, p. 253). Another characteristic is captured by a functional differentiation between manual and automated control activities, *isManual*. Control means may be linked to indicators, *Indicator*, measuring the outcome of actions associated with a particular control means (Frank et al. 2009). In the following, we discuss further design issues with regard to the proposed language design and outline potential paths for future research.

5.3 Design issues and options

Involvement of organisational roles

A main design issue relates to the different types of involvement that organisational roles, i.e., stakeholders, can have in relation to a control objective. The domain analysis suggests further differentiating the involvement of organisational roles. For instance, the IT Governance Institute suggests four types of involvement in the COBIT specification as RACI charts (IT Governance Institute 2007): Responsible, Accountable, Consulted, and Informed. Thus, the conceptualisation of the relation between roles and control objectives in Fig. 5 will probably not be sufficient for audit risk assessment purposes as it lacks elaborate semantics. Figure 7 illustrates two design alternatives that are feasible to represent different types of involvement: First, for each identified type of involvement a particular association between the metatypes representing the organisational role and the control objective could be specified (cf. Fig. 7a). The second option introduces a metatype as an 'association class' between organisational role and control objective and allows for instantiating these four—and further—involvement types as

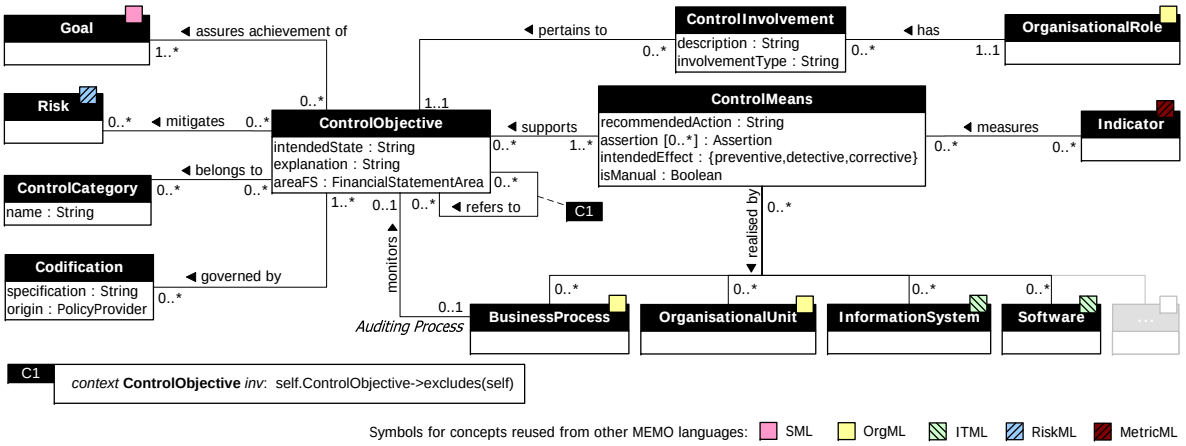


Figure 8: Tentative language design: Working draft of a DSML for internal controls modelling.

associations (cf. Fig. 7b). While the first alternative restricts modelers to predefined types of involvement and their predetermined min/max-multiplicities—and is thus likely to promote a more secure modelling, the second alternative provides more flexibility for language users to add situation-specific relations (e.g., 'supports') without adapting the metamodel. At the stage of language design and regarding the lack of experiences with language use, a combination of both alternatives promises to account for both secure modelling and flexibility. The language design then has to be revised at a later point in time when repeated language application has provided feedback from prospective users—a general consideration pertaining to all design decisions discussed in the present work.

Control Categories

Another design issue pertains to representing categories of controls and to assigning a control to one or more categories, such as 'General', 'Application' or 'IT' control. For the language design, it has to be decided whether a fixed enumeration of categories is built into the language (promoting safe and convenient modelling) or if the language user has to supply categories (promoting flexibility). The decision depends on the availability of a generally accepted categorisation of controls. Such a nomenclature currently only seems to exist for broad categories such as general controls and application controls (Elder et al. 2010, p. 372) while, at the same time, numerous further approaches to subcategorising are being used (e.g., Dunn et al. 2005, pp. 441ff.). Thus, a fixed number of categories built into the language is likely to fail in language applications. Moreover, a control objective can be associated to several reference objects (via *ControlMeans),* which might entail an ambiguous categorisation. We therefore decided to provide a metatype, *ControlCategory*, which allows for creating and assigning one or more categories to a control (cf. Fig. 8).

Monitoring and auditing processes

So far, we have abstracted from the monitoring and auditing processes associated with audit risk assessment (cf. Fig. 2). In principle, those processes combine characteristics of business processes and of projects: They consist of a set of activities following a control flow (e.g., sequence, concurrency and alternative) and are performed by organisational units (usually internal or external auditors). However, an initial analysis of such audit processes reveals a peculiar 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.

In a sense, audit processes are, therefore, associated with the specific audit object(s). However, present process modelling approaches, to our knowledge, do not provide modelling constructs to represent such qualified associations between processes (e.g., a process type 'controls' or 'audits' another business process type). 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 utilise those business process modelling approaches for modelling auditing and monitoring processes that provide time-related events. As the MEMO Organisation Modelling Language (MEMO OrgML) includes differentiated concepts for temporal events, it seems feasible to reuse the *BusinessProcess* concept as is indicated in Fig. 8 by the role *Auditing Process*. The metamodel in Fig. 8 consolidates the discussed design decisions and provides a foundation for future work on internal controls modeling.

6 Conclusion

This paper investigates the potentials of an enterprise modelling approach to audit risk assessment and develops conceptualisations for modelling constructs as enhancements to enterprise modelling to support audit risk assessment. The approach is based on the observation that enterprise models provide a substantial foundation for audit risk assessment in that they represent the organisational 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 modelling—beyond business process modelling. 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 modelling language for audit risk assessment by reflecting key considerations and decisions pertaining to internal controls modelling.

In this paper, we focus on language concepts, especially with regard to the internal control system, its justification, and implementation (cf. Req. 2–4). We discuss design alternatives for corresponding modelling constructs as part of a design research project to develop a comprehensive enterprise modelling 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 a descriptive notation and 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. 4). 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 modelling tool that implements both the enterprise modelling method as well as the control-related enhancements. In this regard, the prolegomena in the present work mark a further step toward an enterprise modelling method in support of audit risk assessment. Such a method and corresponding tool support (Gulden and Frank 2010) remains on our research agenda.

References

Alencar P., Boritz J. E., Carnaghan C. (2004) The relative merits of diagrammatic versues textual representations: a literature review of theoretical and empirical perspectives. Working Paper. University of Waterloo

Alencar P., Boritz J. E., Carnaghan C. (2008) 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. American Accounting Association Los Angeles, CA

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

Bailey, Jr. A. D., Han K. S., Stansifer R. D., Whinston A. B. (2000) The Intelligent Internal Accounting Control Model using a Logic Programming Approach. In: Vasarhelyi M. A., O'Leary D. (eds.) Artificial Intelligence in Accounting and Auditing: Creating value with AI vol. 5. Rutgers Series in Accounting Information Systems. Markus Wiener Publishers, Princeton, NJ, pp. 66–93

Bradford M., Richtermeyer S. B., Roberts D. F. (2007) System Diagramming Techniques: An Analysis of Methods Used in Accounting Education and Practice. In: Journal of Information Systems 21(1), pp. 173–212

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

Cendrowski H., Martin J. P., Petro L. W. (eds.) The Handbook of Fraud Deterrence. John Wiley and Sons, Hoboken, New Jersey

Chen K. T., Lee R. M. (2003) Knowledge-based evaluation of internal accounting control systems — a pattern recognition approach. In: Proceedings of the American Accounting Association Conference. Honolulu, HI

COSO (Sept. 1992) Internal Control — Integrated Framework. Last Access: The Committee of Sponsoring Organizations of the Treadway Commission

COSO (Sept. 2004) Enterprise Risk Management – Integrated Framework (Executive Summary)

COSO (2009) Guidance on Monitoring Internal Control Systems: Introduction. http://www.coso.org. Last Access: The Committee of Sponsoring Organizations of the Treadway Commission

COSO (Sept. 2010) What is internal control? http://www.coso.org/resources.htm

Crawford M., Stein W. (2002) Auditing Risk Management: Fine in Theory but who can do it in Practice? In: International Journal of Auditing 6(2), pp. 119–131

Damianides M. (2005) Sarbanes-Oxley and IT Governance: New Guidance on IT Control and Compliance. In: Inf. Sys. Manage. 22(1), pp. 77–85

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

Dunn C. L., Gerad G. J. (2001) Auditor efficiency and effectiveness with diagrammatic and linguistic conceptual model representation. In: International Journal of Accounting Information Systems 2, pp. 223–248

Dunn C. L., Cherrington J. O., Hollander A. S. (2005) Enterprise Information Systems: A Pattern-Based Approach, 3. ed., internat. ed.. McGraw-Hill Irwin, Boston, MA

Elder R. J., Beasley M. S., Arenes A. A. (2010) Auditing and Assurance Services: An Integrated Approach, 13th ed. Pearson, Boston et al.

Ferstl O. K., Sinz E. J. (1998) SOM Modeling of Business Systems. In: Bernus P., Mertins K., Schmidt G. (eds.) Handbook on Architectures of Information Systems. Springer, Berlin, pp. 339–358

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

Frank U. (2002) Multi-Perspective Enterprise

Modeling (MEMO): Conceptual framework and modeling languages. In: Proceedings of the 35th Annual Hawaii International Conference on System Sciences (HICSS). Honolulu, pp. 72–82

Frank U. (2008) 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

Frank U. (2010) Outline of a Method for Designing Modelling Languages. ICB Research Report 42. Institute for Computer Science and Business Information Systems, Duisburg-Essen University. Essen, Germany

Frank U., Heise D., Kattenstroth H. (2009) Use of a Domain Specific Modeling Language for Realizing Versatile Dashboards. In: Tolvanen J.-P., Rossi M., Gray J., Sprinkle J. (eds.) Proceedings of the 9th OOPSLA workshop on Domain-Specific Modeling (DSM). Helsinki Business School, Helsinki

Gelinas U. J., Dull R. B. (2010) Accounting Information Systems, 8th ed. South-Western Cengage Learning, Mason, OH

Gelinas U. J., Sutton S. G., Fedorowicz J. (2004) Business processes and information technology. South-Western Thomson Learning, Mason, Ohio

Governatori G., Milosevic Z., Sadiq S. (2006) 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. IEEE Computer Society, Los Alamitos, CA, USA, pp. 16–20

Governatori G., Hoffmann J., Sadiq S. W., Weber I. (2008) Detecting Regulatory Compliance for Business Process Models through Semantic Annotations. In: Ardagna D., Mecella M., Yang J. (eds.) Business Process Management Workshops. vol. 17. Lecture Notes in Business Information Processing Springer, pp. 5–17

Gulden J., Frank U. (2010) MEMOCenterNG – A Full-featured Modeling Environment for Organization Modeling and Model-driven Software Development. In: Soffer P., Proper E. (eds.) Proceedings of the CAiSE Forum (Short Papers and Tool Demonstrations) of the 22nd International Conference on Advanced Information Systems Engineering (CAiSE'10), Hammamet, Tunisia, June 7–11, 2010. vol. 592. CEUR Workshop Proceedings Springer, Berlin, pp. 76–83

ISACA (2009) IS Standards, Guidelines and Procedures for Auditing and Control Professionals Information Systems Audit and Control Association Rolling Meadows

IT Governance Institute (ed.) CobiT 4.1: Framework, Control Objectives, Management Guidelines, Maturity Models. IT Governance Institute of the Information Systems Audit and Control Association, Rolling Meadows

Karagiannis D. (2008) A Business process Based Modelling Extension for Regulatory Compliance. In: Multikonferenz Wirtschaftsinformatik., pp. 1159–1173

Karagiannis D., Mylopoulos J., Schwab M. (2007) Business Process-Based Regulation Compliance: The Case of the Sarbanes-Oxley Act. In: Requirements Engineering. IEEE, pp. 315–321

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

Lu R., Sadiq S. W., Governatori G. (Apr. 19, 2009) Measurement of Compliance Distance in Business Processes. In: Inf. Sys. Manag. 25(4), pp. 344–355

Maijoor S. (2000) The Internal Control Explosion. In: International Journal of Auditing (4), pp. 101–109

McCarthy W. E (1979) An entity-relationship view of accounting models. In: The Account-

ing Review 54(4), pp. 667–686
McCarthy W. E (1982) The REA accounting model: A generalized framework for accounting systems in a shared data environment. In: The Accounting Review 57(3), pp. 554–578
Moeller R. R. (2008) Sarbanes-Oxley Internal Controls : Effective Auditing with AS5, CobiT and ITIL. John Wiley & Sons, Hoboken, NJ
Namiri K., Stojanovic N. (2007a) A formal approach for internal controls compliance in business processes. In: 8th Workshop on Business Process Modeling, Development, and Support, BPMDS 2007 in conjunction with CAiSE 2007. Trondheim, Norway
Namiri K., Stojanovic N. (2007b) Pattern-based design and validation of business process compliance. In: Proceedings of the 2007 OTM Confederated International Conference on On the move to meaningful internet systems: CoopIS, DOA, ODBASE, GADA, and IS-Volume Part I. Springer, pp. 59–76
Ortner E. (2008) Language-critical Enterprise and Software Engineering. In: Proceedings of the Fourteenth Americas Conference of Information Systems, AMCIS 2008, Toronto, ON, Canada, Aug 14–17, 2008.
Pitthan J., Philipp M. (Mar. 1997) Einsatz von Petri-Netzen für die Aufnahme, Dokumentation und Analyse Interner Kontrollsysteme im Rahmen der Jahresabschlußprüfung. In: Stucky W., Winand U. (eds.) Petri-Netze zur Modellierung verteilter DV-Systeme. 350. Universität Karlsruhe, Karlsruhe, Germany, pp. 87–104
PricewaterhouseCoopers (July 2004) Sarbanes-Oxley Act: Section 404 — Practical Guidance for Management
Ramos M. (Oct. 2004) Section 404 Compliance in the Annual Report. In: Journal of Accountancy (10), pp. 43–48
Rikhardsson P., Best P., Green P., Rosemann M. (2006) Business Process Risk Management, Compliance, and Internal Control: A Research Agenda. Department of Business Studies, Management Accounting Research Group, Aarhus School of Business. Aarhus, Denmark
Sadiq S. W., Governatori G., Namiri K. (2007) Modeling Control Objectives for Business Process Compliance. In: Alonso G., Dadam P., Rosemann M. (eds.) BPM 2007. vol. 4714. Lecture Notes in Computer Science Springer, Berlin, pp. 149–164
Scheer A.-W. (1992) Architecture of Integrated Information Systems : Foundations of Enterprise Modelling. Springer, Berlin
Scheer A.-W. (2000) ARIS : Business Process Modeling, 3rd ed. Springer, Berlin, Heidelberg
Spira L. F., Page M. (2002) Risk Management — The reinvention of internal control and the changing role of internal audit. In: Accounting, Auditing & Accountability Journal 16(4), pp. 640–661
Strecker S., Heise D., Frank U. (2010) RiskM: A multi-perspective modeling method for IT risk assessment. In: Information Systems Frontiers. Accepted for publication in the Special Issue on Governance, Risk and Compliance Applications in Information Systems
Sutton S. G., Hampton C. (2003) Risk assessment in an extended enterprise environment: Redefining the audit model. In: International Journal of Accounting Information Systems 4(1), pp. 57–73
Westerman G., Hunter R. (2007) IT Risk: Turning Business Threats into Competitive Advantage. Harvard Business School Press, Cambridge

Stefan Strecker, David Heise, Ulrich Frank
Information Systems and Enterprise Modelling
Research Group, Institute for Computer Science
and Business Information Systems (ICB)
University of Duisburg-Essen
Universitaetsstr. 9, 45141 Essen, Germany
<firstname>.<lastname>@uni-due.de