Towards an Empirically Grounded Conceptual Model for Business Process Compliance

Martin Schultz

Chair for Information Systems, University of Hamburg, Hamburg, Germany

martin.schultz@wiso.uni-hamburg.de

Abstract. With the ever increasing number of legal requirements, ensuring business process compliance is a major challenge for today's organizations. Thus, compliance management gained momentum in academia and practice in recent years. Information systems (IS) researchers focus on methods providing automated support for managing diverse compliance requirements. Thereby, compliance is approached from a rather technical perspective. Little effort has been devoted to establish a comprehensive conceptualization of compliance. In particular, previous research neglected to rigorously consider stakeholders' perception based on empirical research. To close this gap, this paper presents an empirically grounded conceptual model for compliance in the context of business processes. Based on results of 17 expert interviews and an online survey, a conceptual model is constructed. The model takes into account the wide range of control means that are applied in organizations to assure compliance. Hence, the model contributes to reducing complexity and improving transparency of the compliance domain.

Keywords: Conceptual model, business process compliance, internal controls

1 Introduction

Nowadays, organizations face the challenge of managing compliance to a steadily increasing number of rules and regulations in their everyday business operations. The rules range from voluntary norms and standards to directives imposed by active legislations. All these compliance rules significantly influence the way organizations design and execute their business processes (BP) [1]. Not surprisingly, practitioners and researchers from the process management domain (BPM) attach more importance to compliance [1]. The vast number of compliance rules and the increasing complexity of BPs in today's organizations require an (semi-)automated support for managing compliance obligations in a cost effective way [2], [3]. This especially holds true in competitive market environments where organizations strive for comprehensive standardization and automation of their BPs by extensively relying on IS. Enterprise resource planning (ERP) systems and accounting information systems (AIS) are widely used to process and store thousands and millions of business transactions each day. Hence, IS researchers have developed (semi-) automated, model-based compliance

adfa, p. 2, 2011.

checking approaches: compliance rules are formally defined and applied to BP models and instances [3]. These approaches consider compliance from a rather technical perspective. However, managing compliance not just involves model checking for several reasons. 1) Compliance rules can become complex, are vague and require interpretation [2]. 2) Organizations take a multitude of different measures to ensure compliance. These measures constitute a complex and interwoven system – a so called internal controls system (ICS) – that involves diverse stakeholders with varying perspectives and acting on multiple organizational levels [4]. 3) Compliance is closely linked to other organization-wide activities like corporate governance or enterprise risk management [5]. However, so far little attention has been paid to address these aspects in IS and BPM research. In particular, only few attempts have been made to conceptualize key concepts of compliance in the context of BPs [2]. This impedes a mutual understanding among stakeholders and hampers a proper formal representation as basis for designing meaningful IS support. Against this background, Sadiq (2011) identifies a "(…) well-grounded conceptual model for compliance and risk" as key issue on the research agenda for BP compliance (BPC) [2].

To close this gap, this paper outlines a conceptual model for BPC considering key concepts from an auditors' perspective as a main stakeholder of compliance. Special attention is paid to the interrelations between compliance and BP models. The design of the model is grounded on empirical research results derived from 17 expert interviews with process auditors [6] and a subsequent online survey [7] as well as a literature review of seminal research work on compliance in the IS and BPM domain.

The remainder of this paper is structured as follows. The next section outlines the related research work regarding key concepts of BPC. Section three explains the applied research method. The results of a domain analysis and related insights gained from earlier empirical research work are presented in section four. In section five the conceptual model is described. A conclusion closes the paper.

2 Related Work

Few seminal research work attempt to conceptualize compliance related concepts and their relations to BPs. Rosemann and zur Muehlen (2005) are among the first to consider the concept *risk* in the context of BP modelling [8]. They link *risk* to a generic conceptual model for BPs and provide a taxonomy of risk types. A model for BPC presented by Namiri and Stojanovic (2007, 2008) includes the concepts *risk, significant account, control objective, control*, and *recovery action* [9], [10]. In this model, a *control* is linked to a *process activity*, a *user*, and a *business document* which are later subsumed as so called *controlled entities*. Furthermore, a *control* mitigates a *risk* respectively supports a *control objective*. For each *control* at least one *recovery action* is defined. Different types of control are distinguished (company level control, IT control, Application control). Karagiannis et al. (2007) present a solution for Sarbanes-Oxley Act reporting requirements and consider *risk, control* and *account* as domain specific concepts. These are linked to *BP elements* (including IS, BP activity, organizational unit). *Control objective, control* and *risk* are also set in relation by Lu

et al. (2008) [11]. Similarly, Strecker et al. (2011) stress *control objective* and *control means* as main concepts in a conceptual model for an internal control system [4]. *Control objectives* are linked to *risk*, *goal* and *codification*. *Control means* support a *control objective* and are realised by a BP, organizational unit, and/ or IS. The concepts are introduced as an extension to an existing enterprise modelling approach. Sadiq et al. (2007, 2009, 2010) use the concepts *control objective*, *internal control*, as well as *risk* and relate these to *process*, *task*, and *property* for an ontological alignment between compliance and the BP domain [12], [13], [14]. Schumm et al. (2010) present a rather abstract conceptual model focusing on *compliance requirements* that stem from a *compliance source*, relate to a *compliance risk* and can be assessed by a *compliance request* [15]. A *compliance requirement* can be addressed by a *control* that is formally expressible as a *compliance rule* and refers to an abstract *compliance target* (BP, BP element). A similar model is presented by Turetken et al. (2011) [16]. Table 1 summarizes the key concepts identified in earlier research work.

Table 1. Overview of domain specific concepts for BPC in related work

Domain Concept	Mentioned by Authors								
	Muehlen (2005)	Namiri (2007)	Namiri (2008)	Karagiannis (2007)	Sadiq (07/09/10)	Lu (2008)	Schumm 2010	Strecker (2011)	Turetken (2011)
Control Objective/ Compliance Requirement		●			●	●	●	●	●
Risk	●	●	●	●	●	●	●	●	●
Compliance Source/ Codification							●	●	●
Compliance Target/ Controlled Entities		●					●		●
Compliance Rule							●		●
Control (Means)		●	●	●	●	●	●	●	●
Recovery Action		●							
Compliance/ Risk Assessment/ Request		●	●				●	●	●
Compliance Fragment							●		
Compliance Concern									●
Business Process	●	●	●	●	●	●	●	●	●
BP element (activity, document, user, IS)	●	●		●	●			●	
Goal	●							●	
Financial Account		●	●	●					

3 Research Method

The research presented in this paper follows the design science approach [17]. The designed artefact is a conceptual model comprising relevant concepts of BPC and their relations. In earlier work we applied a multi-method research approach by combining a qualitative (expert interviews) and a quantitative (online survey) research method to rigorously identify key concepts of the domain from a stakeholder point of view. Regarding the construction of the model, we explicitly elaborate on specific design decisions to ensure transparency. The relevance of the artefact stems from the fact that methods for managing compliance in a cost effective way is an urgent need of many organizations [2], [3]. However, a well-grounded conceptual model as basis for developing appropriate methods and IS support is still missing [2].

There is a consensus in literature that evaluating a designed artefact is an essential step in design science research. As an initial evaluation step the conceptual model is used to design another IS artefact for auditors. Due to page limitations the evaluation is not included in this paper. The evaluation will be supplemented by future research.

4 Domain Analysis

4.1 Terminological Analysis

Designing a conceptual model presupposes the reconstruction of key terms and concepts of the targeted domain [4]. In a broad perspective, compliance describes a state of an organization regarding the conformance to a set of regulations and rules or represents a process to ensure this conformance. The norms originate from a wide range of sources ranging from laws and regulatory requirements to internal guidelines [16], [18]. Compliance is closely linked with the ICS an organization has to maintain. Internal control is broadly defined as a process designed to provide reasonable assurance regarding the achievement of objectives in three categories: 1) effectiveness and efficiency of operations, 2) reliability of financial reporting, and 3) compliance with applicable laws and regulations [19]. It is a system of integrated elements like people, organizational structures, processes, and procedures and therefore covers procedural as well as structural aspects [4]. Key concepts are control objectives and control means. A control objective describes a desired state of an organization or a process and is associated with a recommended course of action that should be taken (control means) to ensure that a control objective is achieved. Control means may involve policies, procedures, practices (e.g. reviews, checks) as well as organizational structures (e.g. authorizations, roles, organizational units) [4], [19], [20].

Audit standards distinguish between process-integrated and process-independent control means (e.g. internal audit function of an organization) [20]. Process-integrated means are further specified as organizational means and control means. Organizational means are preventive security measures that are integrated in the organizational and operational structure of an organization e.g. restricted access, segregation of duties (SoD), approval levels. Control means in this context are measures that are directly integrated in the sequence of operations and constitute e.g. check for completeness or validity [20]. In this procedural sense, a control means represents a target/actual performance comparison enacted as a preventive or detective activity in a process [21]. The terminological analysis reveals that the term control means is subject to terminological ambiguity as it denotes not only procedural but also structural aspects [4]. This is a notable differentiation that is covered in audit standards but so far not comprehensively considered in IS-related literature concerning BPC.

Another core concept strongly related to compliance is risk. Risk can be broadly described as a threat to the achievement of entity's goals/ objectives. To measure risks probability of occurrence and impact of a threat are usually used. A risk has reference objects for which organizational goals are set (e.g. BP) [8], [19], [22]. The relation between risk and compliance is twofold. On the one hand, compliance requirements often directly refer to specific risks. At the same time, compliance requirements intro-

duce a new risk, namely the risk of non-compliance or compliance risk [18]. On the other hand, control objectives are defined and control means are implemented to mitigate risks by reducing their probability of occurrence and/ or their impact.

Compliance is also closely related to the audit domain. Auditing an organization's compliance is often a legal requirement, i.e. annual audits of the financial statements. As audit standards enforce an in-depth analysis of the organization's operations, BPs constitute a central audit subject. Auditors focus on the ICS of an organization as well-controlled BPs contribute to a compliant state of an organization [20].

4.2 Results of Empirical Domain Analysis

For integrating rigorous empirical evidence in the construction process of a conceptual model for compliance, we conducted 17 semi-structured expert interviews and a subsequent online survey (370 respondents) among internal and external auditors [6], [7]. By doing so, we applied a multi-method research approach to determine their understanding on key concepts in the context of process audits. Methodological details on the conducted empirical research are outlined in the respective papers [6], [7].

The results demonstrate a consistent understanding among the auditors regarding the concepts that need to be considered in the context of BPC. 12 concepts are derived: *audit/ control objectives, control means, risk, audit results, standards & regulations, financial statements, materiality, business objectives/ goals, process flow, information systems, organization,* and *data*. These concepts correspond (with partially different terms) to the results of the terminological analysis (section 4.1) and the concepts discussed in related research work (section 2) except the concepts *audit results* and *materiality.* Regarding the concept *control means* the analysis of the empirical data reveals, that auditors consider control means as a special activity in a process that need to be regularly conducted to ensure compliance. The results regarding relations among the concepts are more differentiated. There are only a few relations clearly classified as relevant by the majority of experts and respondents.

5 Conceptual Model for Business Process Compliance

As outlined in section 2, there is consensus on a certain set of concepts that need to be considered when dealing with BPC. Fig. 1 depicts the conceptual model with these concepts identified for the BP and the compliance domain as a class diagram. The model clearly separates these two domains to underline their various relations. This separation facilitates traceability between compliance concepts and related BP concepts [16]. We include the concepts 1) identified as relevant in our empirical work and 2) supported by the majority of authors of related work. Accounting specific concepts (financial accounts/ statements, materiality) are not considered to abstract from specific compliance sources and keep the model generally applicable. The relations are based on the terminological analysis of the domain. In the following the concepts and their relations are briefly described. Specific design decisions are outlined in more detail. From a compliance perspective for BPs a rather generic model can be

assumed consisting of the concepts process (control flow), process activity, and other process elements (organizational resource, data object and IS) [16]. Additionally, the process supports particular organizational goals. The depicted concepts and relations comply with existing meta models for BPs [8]. Using such a generic model ensures that the conceptual model is not restricted to particular BP modelling techniques [16].

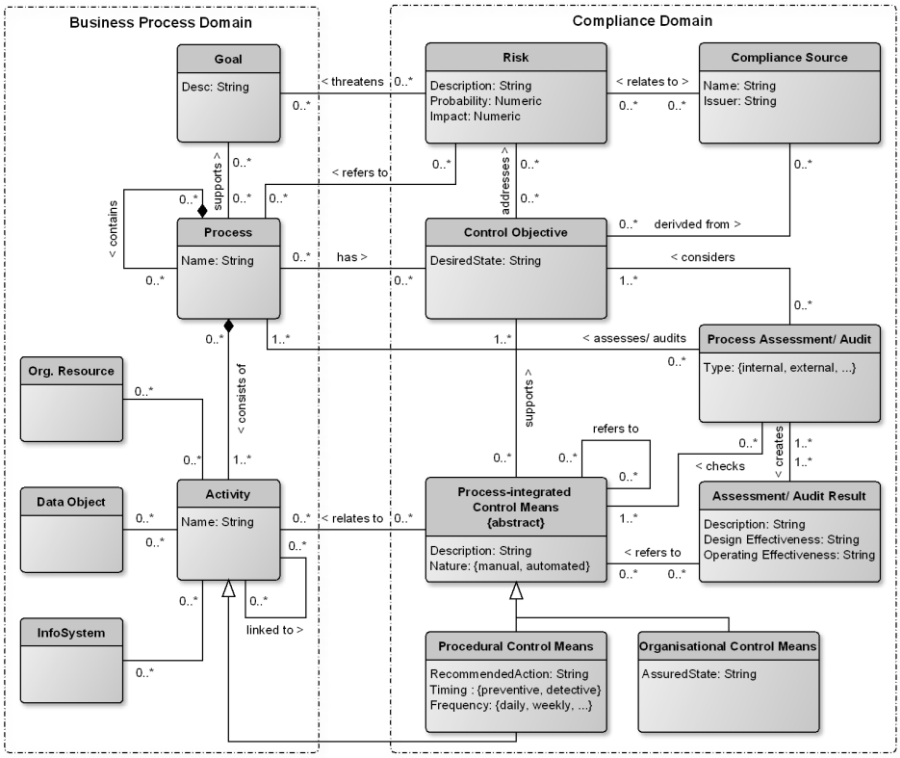

Fig. 1. Conceptual Model for Business Process Compliance

A *Control Objective* describes a desired state of a *Process* and is derived from a *Compliance Source* (e.g. standards, regulations, laws) and/ or addresses a *Risk*. The concepts compliance source and risk are linked to each other as a compliance source can relate to specific risks and might introduce new risks (compliance risks [18]). A risk is linked to a *Goal* as it threatens its achievement. There are one or more *Control Means* supporting a particular control objective. To account for the multiplicity of control means that can be used to achieve a control objective we decide to include an abstract class *Process-integrated Control Means*. The recursive association allows representing control means as interconnected system of control means. In accordance with audit standards, two types of control means inherit from this abstract class [20]. Firstly, *Organizational Control Means* represent all organizational means that can be implemented to ensure compliance, e.g. restricted access, SoD, approval levels. These means refer to requirements that can be easily expresses as a formal rule a process activity has to comply with (e.g. "access to activity X is restricted to appropriate per-

sonnel"). Secondly, *Procedural Control Means* refer to all measures that involve a recommended course of action within the process to ensure compliance (e.g. reconciling sub and general ledger on a weekly basis). These control means significantly differ from the organizational control means as they constitute activities in a particular process. Therefore, this class also inherits from the class *Activity*. Doing so, these control means can be part of a process as a specific type of activity. This conceptual design provides an important link between compliance and BP, reflects the results of the terminological analysis and our empirical results, reduces terminological ambiguity and improves transparency when referring to different types of control means with distinct properties [4]. In a *Process Assessment* of a process related control means are checked against a set of control objectives. An assessment provides an *Audit Result.*

6 Conclusion

Due to an ever increasing number of regulatory requirements today's organizations have to comply with in their daily business, compliance management gained momentum in practice and in academia in recent years. So far, IS researchers consider BPC as rather technical matter and focus on methods to provide (semi) automated support for managing compliance requirements. Only few attempts have been made to establish a comprehensive conceptualization for BPC. Especially, little effort has been devoted to empirical research to rigorously consider stakeholders' perception of this complex domain. To close this gap, this paper presented an empirically grounded conceptual model for BPC. Based on the results of 17 expert interviews and an online survey among internal and external auditors as well as a literature based domain analysis, a conceptual model was constructed. The model takes into account the various types of control means that can be applied to fulfil a certain compliance requirement.

There are several opportunities for further research work. The research presented here is limited to auditors as one stakeholder group for compliance. By considering further stakeholders, valuable new insights could be derived providing a fuller picture of the domain. Similarly, a multi-perspective approach for evaluating the conceptual model contributes to the body of knowledge. This remains on our research agenda.

References

1. Liu, Y., Muller, S., Xu, K.: A static compliance-checking framework for business process models. Ibm Syst. J. 46, 335 –361 (2007).
2. Sadiq, S.: A Roadmap for Research in Business Process Compliance. In: Abramowicz, W., Maciaszek, L., and Węcel, K. (eds.) Business Information Systems Workshops. pp. 1–4. Springer Berlin Heidelberg (2011).
3. Becker, J., Delfmann, P., Eggert, M., Schwittay, S.: Generalizability and Applicability of Model-Based Business Process Compliance-Checking Approaches – A State-of-the-Art Analysis and Research Roadmap. Bur - Bus. Res. 5, 221–247 (2012).
4. Strecker, S., Heise, D., Frank, U.: 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. Enterp. Model. Inf. Syst. Arch. 6, 5–24 (2011).

5. Racz, N., Weippl, E., Seufert, A.: A Frame of Reference for Research of Integrated Governance, Risk and Compliance. In: Decker, B. and Schaumüller-Bichl, I. (eds.) Communications and Multimedia Security. pp. 106–117. Springer, Berlin, Heidelberg (2010).
6. Schultz, M., Mueller-Wickop, N., Nuettgens, M.: Key Information Requirements for Process Audits – an Expert Perspective. Proceedings of the 5th EMISA. pp. 137–150. , Vienna, Austria (2012).
7. Mueller-Wickop, N., Schultz, M., Peris, M.: Towards Key Concepts for Process Audits – A Multi-Method Research Approach. Proceedings of the 10th ICESAL. pp. 70–92. , Utrecht, The Netherlands (2013).
8. Rosemann, M., Muehlen, M. zur: Integrating Risks in Business Process Models. Acis 2005 Proc. (2005).
9. Namiri, K., Stojanovic, N.: Pattern-Based Design and Validation of Business Process Compliance. In: Meersman, R. and Tari, Z. (eds.) On the Move to Meaningful Internet Systems 2007: CoopIS, DOA, ODBASE, GADA, and IS. pp. 59–76. Springer, Berlin, Heidelberg (2007).
10. Namiri, K., Stojanovic, N.: Towards A Formal Framework for Business Process Compliance. Multikonferenz Wirtsch. 2008. 259 (2008).
11. Lu, R., Sadiq, S., Governatori, G.: Compliance Aware Business Process Design. In: Hofstede, A. ter, Benatallah, B., and Paik, H.-Y. (eds.) Business Process Management Workshops. pp. 120–131. Springer Berlin Heidelberg (2008).
12. Sadiq, S., Governatori, G., Namiri, K.: Modeling Control Objectives for Business Process Compliance. In: Alonso, G., Dadam, P., and Rosemann, M. (eds.) Business Process Management. pp. 149–164. Springer, Berlin, Heidelberg (2007).
13. Sadiq, S., Governatori, G.: A methodological framework for aligning business processes and regulatory compliance. Handb. Bus. Process Manag. 2, 159–176 (2009).
14. Sadiq, S., Governatori, G.: Managing Regulatory Compliance in Business Processes. In: Brocke, J. vom and Rosemann, M. (eds.) Handbook on Business Process Management 2. pp. 159–175. Springer Berlin Heidelberg (2010).
15. Schumm, D., Turetken, O., Kokash, N., Elgammal, A., Leymann, F., Heuvel, W.-J. van den: Business Process Compliance through Reusable Units of Compliant Processes. In: Daniel, F. and Facca, F.M. (eds.) Current Trends in Web Engineering. pp. 325–337. Springer Berlin Heidelberg (2010).
16. Turetken, O., Elgammal, A., Willem-Jan van den Heuvel, Papazoglou, M.: Enforcing Compliance on Business Processes through the Use of Patterns. ECIS 2011 Proceedings. , Helsinki (2011).
17. Hevner, A.R., March, S.T., Park, J., Ram, S.: Design science in information systems research. Mis Q. 28, 75–105 (2004).
18. Klotz, M., Dorn, D.W.: IT-Compliance–Begriff, Umfang und relevante Regelwerke. Hmd–praxis Wirtsch. 263, 5–14 (2008).
19. COSO: Internal Control - Integrated Framework, http://www.coso.org, (1992).
20. IAASB: ISA 315 - Identifying and Assessing the risks of Material Misstatement through Understanding the Entity and its Environment. International Auditing and Assurance Standards Board (2009).
21. Sackmann, S., Hofmann, M., Kühnel, S.: Return on Controls Invest. Hmd - Prax. Wirtsch. 289, 31–40 (2013).
22. Strecker, S., Heise, D., Frank, U.: RiskM: A multi-perspective modeling method for IT risk assessment. Inf. Syst. Front. 13, 595–611 (2011).