24th Bled eConference
eFuture:
Creating Solutions for the Individual, Organizations and Society
June 12 - 15, 2011; Bled, Slovenia

A Business Rules Viewpoint on Risk and Compliance Management

Martijn Zoet

HU University of Applied Sciences Utrecht, The Netherlands

martijn.zoet@hu.nl

Johan Versendaal

Utrecht University, The Netherlands

j.versendaal@cs.uu.nl

Pascal Ravesteyn

HU University of Applied Sciences Utrecht, The Netherlands

pascal.ravesteijn@hu.nl

Abstract

Business rules management is a mean by which an organization realizes controllability of business activities to fulfill goals. Currently the focus of controllability is mainly on effectiveness, efficiency and output quality. Little attention is paid to risk, stakeholder concerns and high level goals. The purpose of this work is to present a viewpoint relating business rules management with concepts of risks, stakeholder, concerns and goals. The viewpoint is presented by means of a meta-model existing out of six concepts: stakeholder, concern, goal, business rule, requirements and implementation mechanism. In a case study the proposed view is validated in terms of completeness, usability and accuracy. Results illustrate the completeness, usability and a high degree of accuracy of our defined view. Future research is suggested on the development of a modeling language to improve the communicational value and ease of use of the meta-model.

Keywords: Business Rules Management, Risk Management, Compliance Management, Goal Modeling.

1 Introduction

Business processes fulfill business objectives and goals by executing and coordinating value-adding activities, thereby creating value for the organization (Rikhardsson et al., 2006; Sienou, Lamine and Pingaud, 2008). Historically the focus of business process improvement has been on increasing value by levering efficiency and effectiveness

(Kettinger, Teng and Guha, 1996; Jeston and Nelis, 2006). However, the execution of business processes can lead to the manifestation of risk. Risk, in turn, can reduce value created by business processes and create negative returns. When considering the risk-adjusted value of a business process the overall perceived value to the organization changes (Zur Muehlen and Rosemann, 2005; Rikhardsson et al., 2006; Jallow et al, 2007; Zoet et al., 2009). To prevent the manifestation of risk and preserve added value effective governance needs to be applied. To realize a proper governance structure organizations implement compliance and risk management and business rules management solutions (Ross, 2003; IT Governance Institute, 2007; Tarantino, 2008).

Organizations often consider business rules management and risk management as independent functions and treat them as individual silos (Rikhardsson et al., 2006; Sienou, Lamine and Pingaud, 2008). This approach leads to redundancy, inconsistency, higher cost and increased risk (Open Compliance Group, 2008). Former research has shown that the individual fields are closely related and therefore scientists as well as practitioners are looking for ways to improve the integration between them (Zur Muehlen and Rosemann, 2005; Sienou, Lamine and Pingaud, 2008). Current research can be divided into three distinct areas: architectures, methods and techniques, and modelling languages (Zur Muehlen and Rosemann, 2005; Ghose and Koliadist, 2007; Namiri and Stojanovic, 2007; Sadiq, Governatori and Niamiri, 2007; Kharbili et al., 2008; Sienou, Lamine and Pingaud, 2008). *Architecture* research focuses on the use of specific kind of architectural designs to enforce business rules on business processes thereby realizing compliances. Developed *methods and techniques* mostly focus on analyzing specific types of processes for particular kinds of risk, resulting in process improvements creating a risk-averse or compliant process. On the other hand existing *modeling languages* are extended to deal with specific risk and compliance issues. For example Awad et al. (2009) expand the business process modeling notation (BPMN) such that it can cope with e.g. segregation of duties. A tenet of this paper is that an overall meta-model relating the domains of risk management, compliance management and business rules management can be defined. The purpose of this paper therefore is not to develop a new method, architecture or ontology but provides a way of thinking (viewpoint) that integrates predefined fields. Consequently, in this paper, we address the following research question: How to integrate risk management, compliance management and business rules management, such that it gives a complete, accurate and usable representation for organizations?

Answering this question would help practitioners to better integrate and understand the relationship between risk and compliance management and business rules management (BRM) concepts, while it adds to the scientific body of knowledge by constructing and validating a meta-model for this domain.

The paper is structured as follows. Section 2 discusses the relationship between the risk management, compliance management, BRM presenting a meta-model for integration. Section 3 elaborates on the research methodology and design applied to our research. Section 4 presents the findings and evaluation of the multi-site case study executed. Finally, in section 5 conclusions and suggestions for further research are discussed.

2 Theoretical Foundation

Before presenting the theoretical foundations of our meta-model we want to present the model which summarizes this section, see figure 1 for the meta-model domain integration.

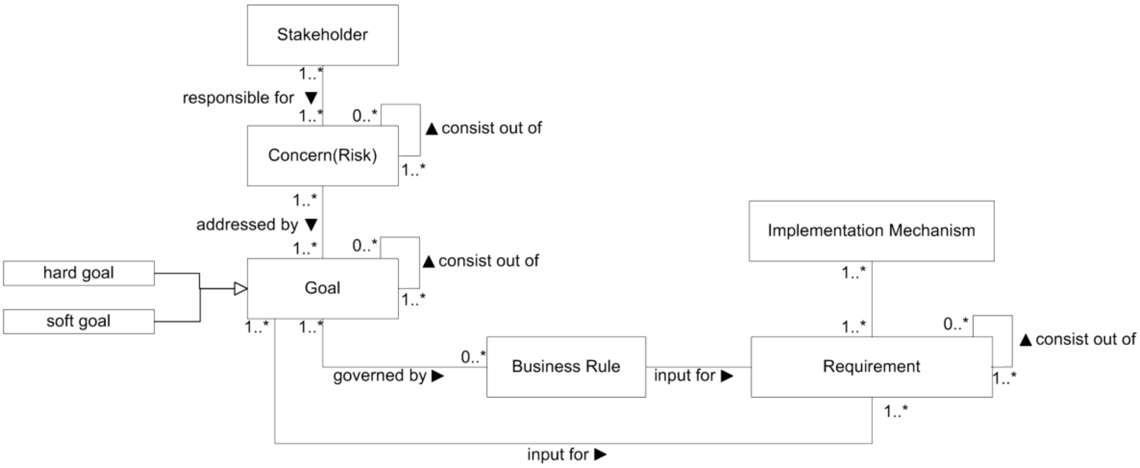

Figure 1: Meta-Model Domain Integration

The creation of the meta-model existed of two steps. First an extensive literature review took place. The units of analysis in our literature review are risk and risk mitigation concepts regarding the design, development or execution of business processes. Databases containing journal articles, working papers, theses, dissertations and conference proceedings were searched using relevant keywords. A particular emphasis was placed on literature in corporate governance, business rules management, risk management and compliance management. The literature review led to an extensive concept matrix of which a cross-section is available in Zoet et al. (2011). Creating the meta-model based on this list would lead to a large and detailed specification enforcing a very strict way of thinking onto organizations. The reason for this is the level at which most concepts are defined namely very specified or even as concept instances. Dealing with brown field situations at most organizations the development of a new detailed way of thinking with a coherent modeling language is not a realistic target. The focus is on leveraging existing concepts and modeling languages such that a coherent view between them arises; the purpose being the alignment of risk and compliance management with BRM. Therefore the second step focused on grouping and translating the concepts and concept instances based on their relationships. After which the concepts were labeled resulting in the eight concepts currently presented in the meta-model. The remainder of this section discusses in brief the origin of the eight concepts.

Organizations apply a broad scope of risk classification labels to distinct the various forms of risk. Examples of such labels are operational risk, financial risk, regulatory risk, compliance related risk, health and safety risk, strategy risk and employee risk management (Tarantino, 2008). Previous research has shown that although many labels exist two main categories of risk can be distinguished, namely compliance risk and operational risk (Zoet et al., 2009). The distinct differences between the two are summarized in table 1.

Causing deviation from an expected outcome and decreasing overall value, compliance and operational risk can be classified as organizational *concerns*. A concern represents a key interest that is crucially important to a specific stakeholder in an organizational system (Open Group, 2009). Examples of concerns, besides risk, are employee satisfaction, profit, customer satisfaction and performance. Concerns can be further decomposed into *sub-concerns*. For example risk can be decomposed into compliance and operational risk and stakeholder satisfaction can be decomposed into profit and stock value.

	Compliance	**Operational**
Source	Laws, regulations, protocols, standards and specifications	Internal strategic, tactical and operational decisions
Risk base is established by	External Parties	Internal Parties
Prove	Based on external criteria	If defined based on internal criteria

Table 1: Overview difference compliance and operational risk

The inability of organizations to properly manage concerns can lead to decreasing overall organizational value. Therefore stakeholders are appointed to govern one or more specific concerns. We first present a definition of a stakeholder derived from Freeman (1984), Jones (1995) and Open Group (2009): a stakeholder is an individual, team, or organization or classes thereof with interest in, or concerns relative to, elements that can affect or are affected by achievements of the organizational system. Stakeholders can be addressed by real names, function names, team names or organization names. Risk concerns originally are appointed to stakeholders based on the type of risk (Aabo, Fraser and Simkins, 2005). Information technology risk is the concern of the IT-department; financial risks are the concern of the finance department et cetera. The last years a paradigm shift is occurring from silo based risk approaches to enterprise risk management (Aabo, Fraser and Simkins, 2005; Tarantino, 2008). The enterprise risk management paradigm treats risks based on event identification instead of silo based identification. By focusing on event based identification the responsibility of governing risk concerns shifts from predefined silos to (operational) stakeholders such as process owners and/or functional, business, project and program managers (Aabo, Fraser and Simkins, 2005; Tarantino, 2008). In addition specific stakeholders such as the CEO, CFO, CIO and senior managers still are appointed to govern specific risk concerns but their focus has shifted from overall risk management to mainly strategic risk concerns. Summarizing, the paradigm shift caused an increase in risk concern stakeholders that all must provide proper governance within their area of responsibility.

Stakeholders tasked with governing risk concerns need to indentify, quantify and mitigate the occurrence or impact. Therefore based on analysis of the as-is situation a to-be situation needs to formulated. In literature multiple concepts to express a to-be situation are indentified namely: strategy, tactic, mission, goals and objectives (Lamsweerde, 2008; Object Management Group, 2010). Although small differences exist, from a goal perspective all previous elements can be considered as different representation layers of the *goal* concept (Object Management Group, 2010). Goals represent some end that one or more stakeholders want to achieve (Open Group, 2009). The achievement itself cannot always be quantified with (exact) measurements; such goals are called *soft goals* (Yu, Strohmaier and Deng, 2006; Lamsweerde, 2008). Soft goals represent concepts such as strategy, tactic and mission. Examples of soft goals are compliance to Basel III, compliance to the Sarbanes-Oxley Act and an implementation of a just-in-time strategy. *Hard goals* can be quantified with measurements that specify its achievement (Yu, Strohmaier and Deng, 2006; Lamsweerde, 2008). To measure the achievement of soft goals typically these need to be refined into one or more hard goals. For example, a bank defining the soft goal “compliance to the customer due diligence guidelines of the Basel committee.” This can be measured by defining multiple hard goals such as “establish a systematic procedure for indentifying new customers”.

Goals state the end that a specific stakeholder wants to achieve. To prevent actors, activities or processes in the organization significantly deviating from desired goals (behaviors), organizations define *business rules* (Morgan, 2002; Debevoise, 2005). A business rule is defined as: “a statement that defines or constrains some aspect of the business with the intention to assert business structure, or to control (influence) the behaviour of the business (Morgan, 2002).” Business Rules therefore constrain the possibilities one has to execute a task and thereby reach a predefined goal. This establishes a higher degree of certainty on how a task is being performed (Bajec and Kripser, 2005; Zur Muehlen and Indulska, 2010). To alter behavior of individuals performing tasks and change the outcome of the activities, organizations need to change their business rules (Debevoise, 2005; Zoet et al., 2011).

By defining appropriate business rules the *requirements* of the organizational system are defined. Within (information systems) requirements engineering literature business rules are input for business requirements (Wiegers, 2003). Although business rules affect the behavior within organizations they are declarative by nature and therefore do not state how the actual enforcement is realized (Ross, 2003). For example a business rule at a construction site can state: "a certified security helmet must always be worn". This statement indicates 'what' must happen: a security helmet must be worn. But it does not indicate how this rule must be enforced. For this a (functional) requirement needs to be defined (Ross, 2003; Wiegers, 2003). A functional requirement is a desired property that must be realized by the organizational information system (Wiegers, 2003). In case of the construction site the functional requirement is: "provide security instructions".

To mitigate risk to adhere to defined goals and to comply with defined business rules the requirement needs to be implemented (Marchetti, 2005; Tarantino, 2008). Organizational elements used to implement a specific requirement are called *implementation* mechanisms (Tarantino, 2008; Zoet et al., 2009) or internal controls (Marchetti, 2005; Tarantino, 2008). By realizing the implementation mechanisms the manner in which organizations manage and execute their business processes are altered. The actual changes to the organization’s business processes depend on variables as availability, cost and impact when the mechanism failures (Marchetti, 2005). For example a distinction can be made between preventive and detective control mechanisms (Ghose and Koliadist, 2007; Tarantino, 2008). Preventive controls are controls that prevent risk from occurring, while detective controls identify risk manifestation that already occurred or are occurring. Based on the construction site example control mechanisms for the requirement “provide security information” can be (a) “A warning sign on the entrance of the workplace” or (b) “A porter at the entrance of the workplace that controls everybody” or (c) “an instruction is given to the employees when they are hired”.

3 Research Methodology and Design

A case study methodology was adopted to validate our meta-model. When choosing a case study approach for theory explanation, five guidelines need to be followed (Benbasat, Goldstein and Mead, 1987; Yin, 1994; Dubé and Paré, 2003; Ågerfalk and Fitzgerald, 2008). The guidelines address the unit of analysis, site selection, data collection method, data analysis and exposition.

The unit of analysis when performing a case study can either be an individual person, a group of people, a specific project or decision (Dubé and Paré, 2003). In this study we focus on the application of our meta-model and its use to classify and relate stakeholders, concerns, goals, business rules and requirements. Stakeholders dealing with risk being a phenomenon of general occurrence no critical, extreme or unique case can be identified. We chose for a research design in which multiple organizations are subject of analysis. The main criteria for selecting organizations is that they must have endured risk manifestation resulting from inaccurate process design or execution. A publicly available database recording this kind of risk manifestation since 2003 is provided by the Security and Exchange Commission. Six organizations were randomly selected from a list of 534 organizations and government institutions that reported risk related concerns between 2003 and 2010.

Organization	Industry
Organization 1	Government
Organization 2	Production
Organization 3	Automotive
Organization 4	Entertainment
Organization 5	Technology
Organization 6	Production

Table 2: Organizations involved in validation

The data collection was conducted by analyzing internal documentation and archival records from the individual organizations as well as the Security Exchange Commission (hence SEC). All information needed to validate the meta-model was derived from these documents and additional interviews were conducted to get a better view of issues related to longitude such as changing requirements, goals or business rules. The integrity, completeness and correctness of the documents are governed by law. They demand that the individual organizations, independent auditors and in some cases the SEC have to sign them off (Law Revision Counsel, 2002; Security Exchange Commission, 2010).

The protocol to analyze the data consists of three steps. First the defined risks in the official documentation, presented to the SEC, and the auditors’ reports were identified and derived. On completion of this step also the process that the risk affects was identified as being part of the risk description. Step two consisted of deriving and matching the indentified risks (concerns) to the goals stated by the auditor to mitigate or reduce the risk (level). After the concern (risk) and goals had been matched the related business rules were indentified. The last step was the identification of the requirement and its implementation technique. All steps were executed by means of an a-priori designed coding scheme consisting of the eight concepts in our meta-model.

4 Findings, discussion and evaluation

In this section we elaborate on the data analysis process. We present our overall findings and evaluate the results. Due to space limitations, we cannot show the individual analyses and results of all 103 risk concern situations from the six organizations included in our sample. We limit our discussion by demonstrating the use of the meta-model based on one specific risk-concern situation (from organization 2).

Situation Description: Incorrect Sales Orders Production Organization

Organization 2 is a multi-site corporation that produces and sells goods to three distinct customer types: government institutions, wholesalers and specialists. To provide flexibility to its customers organization 2 allows orders to be placed by a range of media namely electronic data interchange, contracts, letters, email and phone. Electronic data interchange orders are automatically forwarded to the appropriate production department while all other are put into the sales system by an sales employee. Beginning January 2008 the manager of the sales department and the board, notices a steep increase in complaints by its customers. They state that the goods they get delivered are not the goods they ordered. This situation is depicted in table 3.

Concern: Incorrect Sales Orders	
Stakeholder (s)	Manager sales department (process owner).
Business Process	Sales.
Goal	Decrease errors in sales orders.
Business Rule	A sales order must be checked for completeness and correctness before send to production.
Requirement	Introduce additional check in current process
Implementation Mechanism	Human Actor

Table 3: Risk Concern – Incorrect Sales Orders

Results of incorrect entered sales orders are dissatisfied customers and financial losses. Therefore a solution was needed effected immediately. Analyzing this situation leads to the following instantiation of our meta-model. The concern "*incorrect sales orders*" is a responsibility of the sales manager who is the process owner of the sales process. Based on his concern the following goal was stated, "*decrease errors in sales orders*". The business rule defined to realize this goal was "*every sales order must be checked for completeness and correctness before being sent to production*". To realize the business rule the following requirement has been defined "*introduce additional check in current process*". The actual implementation mechanism was the so-called 'four eyes' principle meaning that an additional sales employee checked every order before send to the appropriate production department. The implementation mechanism partly solved the problem but also caused a huge overhead as every order was checked by two sales employees. Therefore the sales manager requested a change regarding the implementation mechanism. It must be changed from a *human actor* to a *build-in check* in the sales system. When using the meta-model to describe this situation it means that only the instantiation of the implementation mechanisms concept changes, this is depicted in table 4 under timestamp 2. While the number of complaints decreased customers were still complaining. After analysis the sales manager concluded that still a small part of the sales orders were incomplete or incorrect but also that customers received newer version of products they ordered. For example a customer ordered technical component version 1.0 while getting technical component version 1.1. After consulting different managers of production departments the following conclusion was stated: Customers ordering version 1.0 of a product which has already been discontinued receive version 1.1 (according to company policy) although they do not want to. Plotting this situation onto our meta-model means a refinement of the original requirements: *check completeness and correctness of order* and *check product assembly possibilities*. The second requirement entails that before the order is sent to production a check must occur whether the order can (still) be produced. The mechanism chosen to implement the requirement is the sales system.

Risk (Concern): Incorrect Sales Orders			
	Timestamp 1	Timestamp 2	Timestamp 3
Stakeholder (s)	Manager sales department (process owner).	No changes	No changes
Business Process	Sales.	No changes	No changes
Goal	Decrease errors in sales orders.	No changes	No changes
Business Rule	A sales order must be checked for completeness and correctness before send to production.	No changes	No changes
Requirement	Introduce additional check in current process	No changes	Introduce additional check in current process
Sub Requirement 1	-	No changes	Check completeness and correctness of order
Sub Requirement 2	-	No changes	Check Product Assembly Possibilities
Implementation Mechanism	Human Actor	Sales System	Sales System

Table 4: Risk Concern – Incorrect Sales Orders over time

The remainder of the section describes our findings in regarding the metrics ‘completeness’, ‘accuracy’, and ‘usability’ with respect to the meta-model.

C**ompleteness.** Completeness is defined as the percentage of real-life situations that can be mapped onto the meta-model. In total 103 situations concerning operational risk have been indentified within the researched organizations. All situations have been coded using an a priori designed coding scheme consisting of the eight concepts in our meta-model. Similarly as the situation description of “*Incorrect Sales Orders*” we were able to map all other 102 situations which leads us to the conclusion that our meta-model can be considered complete.

A**ccuracy.** Accuracy is defined as the precision by which the meta-model captures the reality of the specified situations. This measurement can be determined by analyzing the loss of information when mapping situations to our meta-model. Regarding stakeholders, goals, business rules and requirements, the model captures the full richness of the situation. Information loss does occur when applying the concept of *implementation mechanism* by the degree of rigourness used during the execution of the case studies. We generalized to generic organizational (process) elements such as human actor, system actor, tasks and processes. Thereby loosing, in some cases, detailed information on the exact location of the implementation mechanism. For example some documents stated the exact application interface or component altered, removed or added to fulfill the requirement. One can therefore argue that the accuracy of the meta-model needs to be improved before being usable in practice. Although when further specifying the concept *implementation mechanism* into elements such as application interface, infrastructure service and application services (modeling) language, decisions need to be made. We have to define in detail which implementation mechanisms there are and how they are organized. For example an application consists of components, interfaces and functions. The same can be applied to business process, business services et cetera (see figure 2).

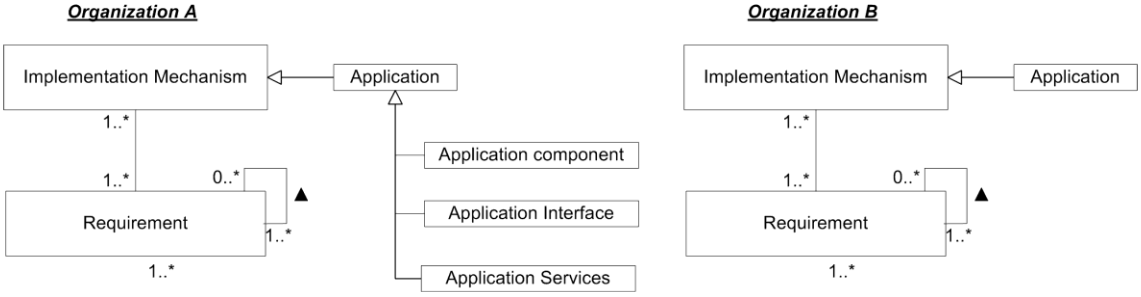

Figure 2: Demonstration level of specification implementation mechanism

As different organizations can use different concepts and modeling languages with different underlying meta-models (see figure 2) a translation would be needed from our meta-model to the one the organization uses. This would defeat the purpose of our meta-model as high-level integration model. Therefore we choose not to further specify the implementation mechanism concept but leave this open to the organization using the meta-model. They can further specify the concept based on the languages and concepts already in use.

Usability. Usability for this study is defined as the combined measurements accuracy and completeness. This measurement can be determined by analyzing the individual measurements combing them and conclude the usability of the model. Executing the case studies has shown that the model can be used to model all identified situations without loss of information for five out of six concepts. Regarding the concept of requirements it has been discussed why we believe the basis meta-model works best while incorporating this loss of information. Therefore we conclude that the meta-model was proven to be usable to realize the integration between the different fields and serve as a starting point to further study of the phenomena.

5 Conclusion and Future Research

In this paper we defined a meta-model in order to answer the research question: how to integrate risk management, compliance management and business rules management, such that it gives a complete, accurate and usable representation for organizations? We elaborated on the difference between operational and compliance risk leading to the conclusion that both are specific risk concerns an organizational stakeholder can be hold responsible for. Additionally we elaborated on the relationship between operational risk, compliance risk, BRM and requirements resulting in the defined meta-model. The meta-model has been tested on 103 situations at six organizations; the paper discussed one particular situation in detail. The research enables us to conclude that our meta-model contributes to the integration of the different fields. While doing so our approach does not contradict or conflict with current languages present in the fields of enterprise architecture or business rules.

This work represents a further step in research on synthesizing risk management, compliance management and BRM. While this work has focused on constructing and validating a meta-model, future research should explore a proper way of presenting, communicating and using the meta-model. A promising approach and direction for subsequent research would be the work of Engelsman et al. (2010), who have created a comparable model (ARMOR). The model has significant differences though. ARMOR does not address business rules, yet it deals with requirements and implementation mechanisms in a more detailed manner thereby aligning with a specific modeling language: Archimate. Recognizing this difference ARMOR might provide a possible modeling language on top of our meta-model.

References

Aabo, T., Fraser, J. & Simkins, B. (2005). The Rise and Evolution of the Chief Risk Officer: Enterprise Risk Management at Hydro One. Journal of Applied Corporate Finance. 17 (3), 18-31.

Ågerfalk, P. & Fitzgerald, B. (2008). Outsourcing to an unknown workforce: Exploring opensourcing as an offshore sourcing strategy. MIS Quarterly. 8 (2), 385–409.

Awad, A., Grosskopf, A., Meyer, A., & Weske, M. (2009). Technical Report: Enabling resource assignment constraints in BPMN. Potsdam: Hasso Plattner Institute. (Report 04-2009).

Bajec, M. & Kripser, M. (2005). A methodology and tool support for managing business rules in organizations. Information Systems. 30 (6), 423-443.

Benbasat, I., Goldstein, D. & Mead, M. (1987). The Case Research Strategy in Studies of Information Systems. MIS Quarterly. 11 (3), 369-385.

Debevoise, T. (2005). Business Process Management with a Business Rules Approach: Implementing the Service Oriented Architecture. Canada: Business Knowledge Architects.

Dubé, L. & Paré, G. (2004). Rigor in information systems positivist case research: current practices, trends and recommendations. MIS Quarterly. 27 (4), 597-635.

Engelsman, W., Quartel, D., Jonkers, H. & Van Sinderen, M. (2010). Extending Enterprise Architecture Modelling with Business Goals and Requirements. Enterprise Information Systems. 5 (1), 9 - 36.

Freeman, R. (1984). Stategic Management: A Stakeholder Approach. Boston: Pitman.

Ghose, A. & Koliadist, G. (2007). Auditing Business Process Compliance. In ICSOC 2007 (169-180). Heiderlberg: Springer.

IT Governance Institute, (2007). Framework Control Objectives Management Guidelines Maturity Models. Rolling Meadows: IT Governance Institute.

Jallow, A., Majeed, B., Vergidis, K., Tiwari, A. & Roy, R. (2007). Operational Risk Analysis in Business Processes. BT Technology. 25 (1), 168 – 177.

Jeston, J., Nelis, J. (2006). Business Process Management - Practical Guidelines to Successful Implementations. Oxford: Butterworth-Heinemann.

Jones, T. (1995). Instrumental stakeholder theory: A synthesis of ethics and economics. Academy of Management Review. 20 (2), 404-437.

Kettinger, W., Teng, J. & Guha, S. (1996). Business Process Change: A Study of Methodologies, Techniques, and Tools. MIS Quarterly. 21 (1), 55-80.

Kharbili, M., Stein, S., Markovic, I. & Pulvermüller, E. (2008). Towards a Framework for Semantic Business Process Compliance Management. In: International Conference on Advanced Information Systems 2008 (1–15). Heidelberg: Springer.

Lamsweerde van, A. (2008). Requirements Engineering: From Craft to Discipline. In ACM Sigsoft International Symposium on the Foundations of Software Engineering. Atlanta.

Law Revision Counsel (2002). Sarbanes-Oxley Act of 2002. 20-12-2009, from http://uscode.house.gov/download/pls/15C98.txt.

Marchetti, A. (2005). Beyond Sarbanes-Oxly Compliance: Effective Enterprise Risk Management. New Jersey: Wiley.

Morgan, T. (2002): Business Rules and Information Systems. Indianapolis: Pearson Education.

Namiri, K. & Stojanovic, N. (2007). A Formal Approach for Internal Controls Compliance in Business Processes. In: 8th Workshop on Business Process Modeling, Development, and Support 2007 (1-9). Trondheim.

Open Compliance Group. (2008). Reports on compliance and risk management efforts. 20-12-2009, from http://www.oceg.org/.

Open Group. (2009). Togaf Version 9. San Francisco: The Open Group.

Object Management Group. (2010). Business Motivation Model (BMM) version 1.1., 06-06-2010, from http://www.omg.org/spec/BMM/1.1/PDF

Rikhardsson, P., Best, P., Green, P. & Rosemann, M. (2006). Business Process Risk Management and Internal Control: A proposed Research Agenda in the context of Compliance and ERP Systems. In Second Asia/Pacific Research Symposium on Accounting Information Systems, Melbourne.

Ross, R. (2003). Principles of the Business Rules Approach. Boston: Addison-Wesley.

Sadiq, S., Governatori, G. & Naimiri, K. (2007). Modeling Control Objectives for Business Process Compliance. In Business Process Management Conference, (149-164). Heidelberg: Springer.

Security and Exchange Commision. (2010). Releases Issued by the SEC on PCAOB Rule Proposals. 06-01-2009, From http://www.sec.gov/rules/pcaob.shtml

Sienou, A., Lamine, E. & Pingaud, H. (2008). A Method for Integrated Management of Process-risk. In International Workshop on Governance, Risk and Compliance: Applications in Information Systems, June 9 (16-30). Montpellier, France.

Tarantino, A. (2008). Governance, Risk, and Compliance Handbook. New Jersey: Wiley.

Wiegers, K. (2003). Software Requirements. Redmond: Washington.

Yin, R.K. (1994). Case Study Research, Design and Methods 2nd edition. Beverly Hills: Sage Publications.

Yu, E., Strohmaier, M. & Deng. X. (2006). Exploring Intentional Modeling and Analysis for Enterprise Architecture. In proceedings of the EDOC 2006 Workshop on Trends in Enterprise Architecture Research, (1-8).

Zoet, M., Welke, R., Ravesteyn, J. & Versendaal, J. (2009). Aligning risk management and compliance considerations with business process development. In: Vol. 5692. Lecture Notes in Computer Science (157-168). Heidelberg.

Zoet, M., Versendaal, J., Ravesteyn, J. & Welke, R. (2011). Alignment of Business Process Management and Business Rules. To be published in 2011 European Conference on Information Systems (ECIS) Proceedings.

Zur Muehlen, M. & Rosemann, M. (2005). Integrating Risks in Business Process Models. In Proceedings of 16th Australasian Conference on Information Systems (1-10), Sydney.

Zur Muehlen, M. & Indulska M. (2010). Modeling languages for business processes and business rules: a representational analysis. Information Systems. 35 (4), 379-390.