Risk Management in the BPM Lifecycle

Michael zur Muehlen and Danny Ting-Yi Ho

Howe School of Technology Management,
Stevens Institute of Technology,
Castle Point on the Hudson, Hoboken, NJ 07030
{mzurmuehlen, tho2}@stevens.edu

Abstract. Business Process Management is considered an essential strategy to create and maintain competitive advantage by streamlining and monitoring corporate processes. While the identification of critical success factors for the management of business process related projects has been addressed by some research projects, the risks associated with these projects have received considerably less attention. This is a concern: Although BPM projects contain phases that relate to traditional software development and deployment projects, the application of risk mitigation strategies found in software engineering ignores the subsequent process management phases that follow upon the implementation and automation of processes. This paper provides an overview of risks associated with BPM projects along the phases of the BPM lifecycle. After a classification of the risks identified with individual lifecycle phases and transitions we discuss four strategies to deal with these risks: avoidance, mitigation, transfer, and acceptance. The outlook of this paper discusses how assessment frameworks such as CobIT and COSO can be applied to risk management in the context of BPM.

1 Motivation

The specification and improvement of corporate processes is a measure that helps functional organizations improve the hand-off points of work items between departments. After the majority of the 1990s reengineering projects put business processes at the center of reorganization strategies, process management has more recently been realigned with continuous improvement efforts that go back to the Total Quality Management initiatives of the 1980s, and continuous improvement efforts that have their roots in W. Edwards Deming's work in the 1950s.

Business Process Management covers the lifecycle of process discovery, specification, implementation, execution, monitoring and controlling. While corporate reorganization often focuses on the makeup of structural entities such as departments and divisions, the core processes enacted to deliver products are services tend to remain a core binding element for organizations. Consequently, structuring organizations around business processes is a popular topic both in management and the technical literature. A study conducted by Grover indicates that, even with enormous time and investment devoted, 7 out of 10 surveyed business process

projects failed [1]. Such a high failure rate implies that in addition to understanding what should to be done in process reengineering projects, the avoidance of things that should *not* be done deserves equal attention. We are particularly interested in describing the risks that endanger the success of business process projects, such as those listed in [2, 3].

In this paper, we describe specific risks that BPM projects are exposed to along the BPM lifecycle. Based on four risk management strategies we discuss the options that a BPM project manager has in dealing with these risks. Finally, we outline the role of existing frameworks such as COSO and CobIT in identifying existing risks and planning for their mitigation.

2   Business Process Management

The general notion of the term business process is widely understood, but there exist almost as many definitions of the term as there are authors writing about the topic. In general, processes transform input into output along a path of activities, which may invoke or consume resources such as people or materials. Depending on the position of the process within the corporate supply chain, core and support processes can be distinguished. Core processes (sometimes called identity processes) are the main value-creating pipelines of an organization; they are triggered by interaction with external parties such as suppliers or customers, and their output is directed at consumers outside the organization. Support processes are mainly internal to an organization, and enable the execution of core processes. They do not produce results that are of direct value to customers or suppliers. To formalize these notions we propose the following definition of a process: A process is a sequence of activities that is necessary to manipulate an object of economic interest to the organization, and that achieves a specific goal. The components of a process are both the structure of the process (i.e. the control flow among activities, data flow dependencies, and business rules that cover constraints in the execution of the process), its goals, as well as ancillary elements such as resources, input and output.

Management in general is a cross-sectional function that controls the use of resources and choreographs the operational activities of the enterprise. Management functions follow a lifecycle of planning, organizing, staffing, directing and controlling, and budgeting. Business Process Management is the application of this management cycle to an organization's business processes. While Business Process Management has gained interest in industry over the last few years (compare e.g. [4]), its roots are not new. For instance, Levin proposed the ideas of automatic process control in physical processes to office work in 1956 [24].

Zairi and Sinclair see BPM as "a structured approach to analyze and continually improve fundamental activities such as manufacturing, marketing, communications and other major elements of a company's operations" [5]. Elzinga et al. emphasize that no matter how continuous improvement is performed, it must be based on the quality of products and services that will be evaluated by the customers. Consequently, they define BPM as "a systematic, structured approach to analyze, improve, control, and manage processes with the aim of improving the quality of

products and services" [6]. Harmon echoes this idea: "BPM refers to aligning processes with the organization's strategic goals, designing and implementing process architectures, establishing process measurement systems that align with organizational goals, and educating and organizing managers so that they will manage processes effectively" [7].

The above definitions all point to the core task of Business Process Management: To create alignment among the individual process components input, output, resources, process structure, and process goals. If such alignment is achieved, the overall process performance of the organization should increase both in terms of process quality (e.g. less waste, idle time, rework) and quantity (e.g. shorter cycle times, faster adjustment to environmental changes). Alignment is seldom achieved through a one-time process. Instead, an iterative approach in form of a continuous process management lifecycle helps organizations achieve, maintain, and improve the quality of their processes. This lifecycle is shown in figure 1.
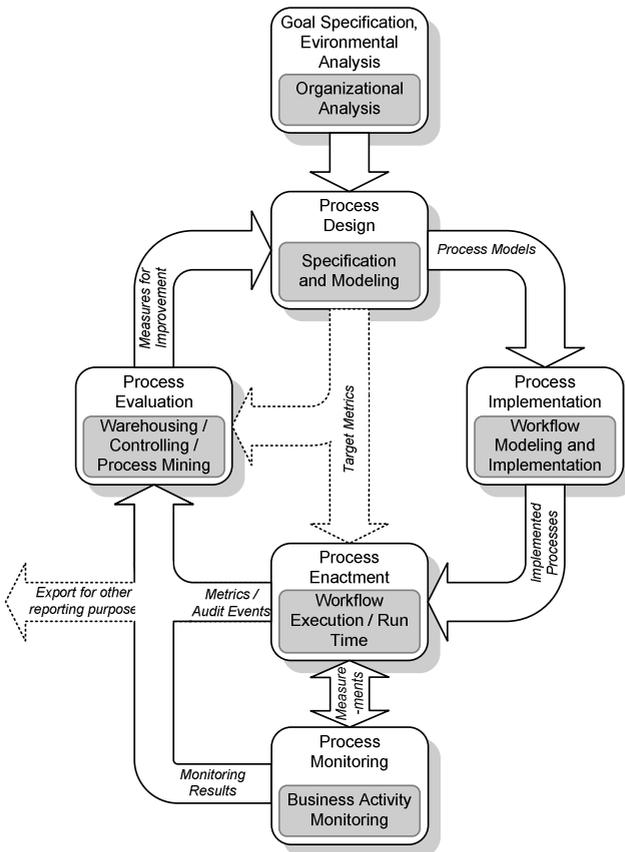

Fig. 1. Business Process Management Lifecycle

The process lifecycle starts with a definition of organizational and process goals, and an assessment of environmental factors and constraints that have an effect on the business processes of an organization. The purpose of the following process design phase is the identification of those processes an organization wishes to analyze, redesign, and/or automate. The details of these processes are specified and mapped using (semi-)formal modeling methods. Before processes are designed or redesigned, it is necessary to identify and clarify variables that will influence the process design. Internally, these variables include the purpose and deliverables of the process, known limitations of the process and the affected organization. External variables reflect the influence of outside parties such as suppliers, customers, competitors and governmental agencies. The completeness of the goal specification and the organizational analysis defines the parameters and thus the constraints for the desired process design.

During the process implementation phase the specified process models are transferred into the operational environments which can either be manual (e.g. via procedure handbooks) or automated (e.g. via BPM or workflow software). Finally, individual process instances are derived from the process specification and executed; their performance is monitored in real time. For the purpose of process control and improvement, audit trails produced during the process enactment and monitoring stages can be used in the evaluation stage. During this stage data from multiple process instances is aggregated to discover temporal trends and design flaws. Feedbacks and contingency plans for process improvement can be formulated based on the results of process measurement and evaluation.

3   Risks and Risk Management

In classical decision making theory, risk is conceived as "reflecting variation in the distribution of possible outcomes, their likelihoods, and their subjective values" [8]. By this definition, risk can be expressed mathematically as "the probability of occurrence of loss/gain multiplied by its respective magnitude." [20] The Project Management Institute defines risk as "an uncertain event or condition that, if it occurs, has a positive or negative effect on a project objective" [23]. Since risks are commonly associated with negative outcomes [8], the distinction between risks and problems often remains unclear. Charette claims that a risk is not a problem, but at most a "potential problem" that may result from making a particular decision. To some extent "risk is the probability of unwanted consequences of an event and decision" [10].

3.1   Risk Management

The purpose of risk management is to "reduce or neutralize potential [risks], and simultaneously to offer opportunities for positive improvement in performance." [22] A general risk management framework is composed of 3 main action phases: identification, analysis, and control [3]. In practice, the risk identification phase is typically conducted by an expert group through brainstorming or techniques such as

fault tree or event tree analysis, cause consequence analysis, or failure mode and effect analysis.

Risks are caused by uncertainties [12], thus it is often difficult to frame risks in a precise fashion. One way to do so is to characterize risks using properties such as impact, probability, time frame, and coupling with other risks [12]. Four risk-handling strategies are suggested in the literature: mitigation [13], avoidance, transfer, and acceptance /assumption [14], table 1 summarizes these strategies in detail.

Table 1. Risk Management Strategies

RISK MGMT. STRATEGY	DEFINITION	EXAMPLES
Mitigation	To reduce the probability of a risk and/or the impact that an occurrence of the risk may bear. Risk limitation aims at the implementation of controls that dampen the effects of risk occurrences, while not completely alleviating them.	• Standardized process routing • Formalized exception handling • Complete kit processing • Collaboration, checks & balances
Avoidance	To eliminate the probability of a specific risk before its occurrence. This strategy is normally realized by trading the risk for other risks that are less threatening or easier to deal with.	• Process redesign
Transfer	To shift risk or the consequences caused by the risk from one party to another. Also called "risk sharing". Risk transfer may involve the purchase of an insurance policy, or the outsourcing of risky project parts.	• Process Outsourcing • Insurance Policies
Acceptance/ Assumption	To adapt to the risk when it becomes a problem. The enactment of a risk contingency plan is required in this strategy.	• Adaptation to regulartory requirements

3.2   Common Taxonomies of Risk in Enterprise Projects

The notion of risk in enterprise projects has been dealt with extensively in the academic literature. The most popular taxonomy of risks in enterprises looks at the risk context. Typically, a business entity is always threatened by natural risks, human risks, and environmental risks [14]. Similarly, in the field of business process management projects, risks can be categorized into three groups: people risks, management risks, and technical risk [3]. Nevertheless, Davenport points to organizational/human resources and information technologies as two major enablers of process innovation [15]. This implies that the enablers of process innovation can produce negative impacts on businesses if they are not managed properly.

In their model of risk factors in Enterprise Systems implementations, Scott and Vessey add external business context to the risk factors identified above [16]. They suggest that risks can produce a positive impact on businesses if they are well

managed within the organization and if the organization is able to react to outside changes. In Sumner's research, the general risk context is broken down into smaller groups: skill mix, management structure and strategy, software system design, user involvement and training, technology planning, project management, and social commitment [17]. Figure 2 provides a taxonomy of risk that was derived from the above sources and a review of risk management literature as provided in [25].

Property	Value			
Cause	External		Internal	
Likelihood	Certain	Highly Probable	Moderately Probable	Improbable
Severity	Loss of asset, capability, process	major delay of process, loss of data	Minor process disruption	Delayed detection of misconduct
Affected Area	Financial	Technical	Functional	Organizational
Cause of Error	Skill-based	Knowledge-based		Rule-based
Detectability	Prior to effect	At time of effect		After the effect

Fig. 2. Taxonomy of risk properties

Risks may originate either from within the organization, or they may be caused by external factors. In the case of BPM projects, examples for these cases are a lack of BPM capabilities among the members of the project team, or the choice of an external supplier that is unable to deliver the required technology. The likelihood of a risk occurrence can range from certain risks, in which case error handling procedures should be in place, to improbable risks. The effects of risk can vary in severity. Some risks may jeopardize the entire BPM effort (e.g. loss of executive support) while others are just a delayed recognition of minor risks, such as documentation or governance issues. The area affected by risk ranges from financial aspects, technical capabilities, functional capabilities, to organizational issues. Risks do not materialize by themselves, but they reflect the outcome of some (intentional or unintentional) mistake. Such mistakes can be caused because the necessary skills are absent, i.e. the project staff is lacking training in the tools and methods applied. They may happen because the knowledge to manage a new context is absent, i.e. if the project staff does not recognize the context of a problem to find an appropriate solution. And finally, the project management rules may force participants to work in a particular fashion that is not suited to mitigate a given problem, in other words, policies and procedures did not allow for proper risk mitigation.

4   Risks Specific to BPM Projects

While the lifecycle shown in figure 1 is the depiction of an ideal continuous process management strategy, its execution is subject to numerous risks that need to be managed. Some of these risks occur within the phases of the lifecycle, while others are specific to the transition between two phases.

The following table lists common risks encountered in and between these phases. The majority of the risks identified lie in a) a mismatch of methods employed in the different phases of the process lifecycle, b) a lack of clarity who is responsible for the individual phases or their results, and c) a mismatch of process design, automation, and evaluation objectives (i.e. goal mismatch). Managers of BPM projects should pay particular attention to these areas.

The lifecycle-based classification of risks in BPM projects is useful from a managerial perspective, as it allows BPM project managers to address specific risks that relate to the current phase of the BPM project, there is some overlap among risks that occur across different lifecycle phases. In order to identify these risks, a more functional classification of BPM project risks is needed. These functional categories cluster risks that have common antecedents, e.g. a lack of training, general project management skills, or technology choices. By managing the common root causes of these risks, a BPM project manager may be able to control more effectively risks that affect several lifecycle phases.

Table 2. Lifecycle-specific Risks in BPM Projects

Lifecycle Phase	BPM-specific Risk
Analysis	• Conduct analysis without a view on enterprise/process/task strategy • Failure to define process goals/values in a language understandable for process stakeholders • Overemphasis of technical variables • Failure to relate systematic/organizational risks to the analysis • Analysis language is not capable to represent observed process semantics
Analysis → Design	• Failure to properly map analysis outcomes to design models • Loss of information during the mapping processes
Design	• Implementation modeling languages are not capable to represent desired process semantics • Design using incompatible modeling technologies • Lack of communication between process designers and process stakeholders • Designers ignore the organizational perspective of process design • Risk handling mechanisms are missing in the design • Modelers use different levels of abstraction
Design → Implementation	• Wrong translation from process models to implementation plans • Mismatch of design method and implementation method/perspective

Implementation	• Lack of a high level implementation view (for executives) • Lack of process management knowledge at the management level • Overemphasis on technical issues • Resulting models do not fit the current infrastructure • Resulting models do not fit the current organizational structure • Failure to relocate resources (plans for transformation) • Failure to rearrange/reassign roles and responsibilities to process stakeholders (instantiate process management) • Process stakeholders assume they know the new processes and their roles without review of the redesign
Execution	• Lack of communication and a common language among stakeholders • Resistance from stakeholders to perform process-oriented activities • Stakeholders take too long to adapt to process-oriented work style • Stakeholders are unable to collaborate across organizational boundaries • Stakeholders feel uncomfortable under process-oriented leadership • The composition of stakeholders changes during the runtime • System is unstable in the runtime environment • Service vendors merge or go out of business • New regulatory requirements make current process practices illegal
Monitoring	• Lack of monitoring strategies, plans, objectives, and methods • Stakeholders/Laws prohibit process transparency (monitoring) • Flawed monitoring information produced by stakeholders • Absence of a precise information filtering policies • Monitoring without a qualitative perspective (i.e. numerical focus) • Monitored objectives differ from original design objectives
Monitoring & Execution → Controlling	• Information overload of monitoring recipients • Failure to translate raw audit data into useful information • Lack of management in merging multiple information channels • Unrecorded human interference in the process • Failure to report critical issues to allow timely response
Controlling	• Missing standards for evaluation policies/methods • Controlling objectives are different from process design objectives • Misinterpretation of audit data • Missing link from audit data to business data • Failure to relate the evaluation to strategic and external variables
Controlling → Design	• Lack of well-defined feedback mechanisms • Inability to recognize problems from process evaluation • Failure to derive contingency plans form the evaluation • Controlling and process improvement conducted by different stakeholders

The following table contains a classification of risk categories that we subsequently apply to the risks listed in table 2. The risk categories described in this table are based on a review of the related literature discussed earlier.

Table 3. Risk Classification

Risk Factor	Definition
Method	Lack of understanding or misuse of methods in the planning, design, implementation, enactment, evaluation phase.
Communication	Lack of communication among BPM stakeholders and participants. This Includes conversations, meeting, training, reporting, and communication in all other forms [3, 17, 18]
Information	Absence of information efficiency, effectiveness, security, flexibility for both transfers between lifecycle phases and process monitoring and controlling efforts. [17, 18]
Change Management	Inability to manage/perform changes [1, 3, 17, 18]
System / Technology	Failure of system/technology implementation due to the system/technology's nature or through improper human interference [1, 17, 18]
Leadership / Management	Failure to display strong leadership and/or proper project management [1, 3, 17]
Resource / Skill	Lack of desired resource/skill sets or the misuse of resources/skills [1, 3, 17, 18]
Strategy	Failure to define vision, goals, functions of all BPM stakeholders, participants, and components involved [1, 3, 17, 18]

Table 4. Mapping of BPM Risks to Risk Taxonomy

Risk Factor	Life-Cycle Risks
Method	• Invalid process analysis/design methods [1], [2] • Invalid mapping methods (problem to solution, solution to implementation) [1, 2], [2, 3] • Invalid process modeling methods [2, 3] • Invalid process implementation methods [3] • Invalid evaluation methods [5] • Inconsistency of evaluation/measurement methods [5], [6] • Invalid feedback mechanism [5, 2]
Communication	• Miscommunication of goals [1,2] • Lack of communication among stakeholders [ALL] • Hidden assumptions in design and implementation [1,2,3]
Information	• Misusage of information [1,2], [4,6], [5] • Inadequate information [ALL] • Invalid information [1, 2], [2, 3], [5, 2] • Invalid information conversion [6, 5]
Change Management	• Failure to redesign jobs/functions [1, 2] • Failure to perform necessary changes [2] • Inability to recognize problems [5, 2] • Inability to react to designated changes [ALL]
System / Technology	• Lacking technology acceptance [ALL] • Misusage of technology [ALL] • Lack of technology flexibility [ALL] • Lack of technology compatibility [ALL] • Lack of technology scalability [ALL]

Leadership / Management	• Lack of leadership/management [ALL] • Inconsistency of leadership/management [ALL] • Absence of leadership/management [ALL]
Resource / Skill	• Absence of resource/skill [ALL] • Misusage of resource/skill [ALL] • Inability to use resource/skill [ALL]
Strategy	• Inaccurate strategic definition [ALL] • Unclear strategic definition [ALL] • Absence of strategic definition [ALL]

Now that we have established a classification for different types of risk, we can map the BPM-specific risks from the previous section to these categories. The numbers behind the lifecycle specific risk example denote the lifecycle phase in which the risk was identified [1=organizational analysis, 2=design, 3=implementation, 4=execution, 5=monitoring, 6=controlling].

A look at table 4 shows that while some of the categorized risks apply to specific lifecycle phases and transitions, all of the risks associated with the categories system/technology, leadership/management, resource/skill, and strategy affect all phases of the BPM lifecycle, i.e. they are orthogonal to the progress any BPM project makes through the lifecycle. Consequently, a BPM project manager should address these orthogonal risks prior to the start of the project, while risks in the other categories are specific to individual lifecycle phases, and may lend themselves to a deferred mitigation approach.

5 Other Approaches to Risk Management: ERM and COBIT

Kliem claims that risk management should consist of three actions: risk identification, risk analysis, and risk control [3]. By the same token, Peltier suggests a complete risk management lifecycle that should include the following key concepts: analysis, design, construction, test, and maintenance [14]. In either case, there is consensus that a lifecycle concept is essential and fundamental to risk management.

ERM is a framework designed by the Committee of Sponsoring Organizations of the Treadway Commission (COSO) that helps businesses assess and enhance their internal control systems. The term "internal control system" includes all policies and procedures that an organization adopts to achieve management's objective of ensuring the orderly and efficient conduct of business [11]. COSO defines ERM as "… a process, effected by an entity's board of directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regard in the achievement of entity objectives" [11]. COSO claims that in order to minimize the impact of risks risk management must address four major areas: strategy, operations, reporting, and compliance. In addition to these areas, eight individual risk components have to be reviewed. These are the internal environment, objective setting, event identification, risk assessment, risk response, control activities, information and communication, and monitoring.
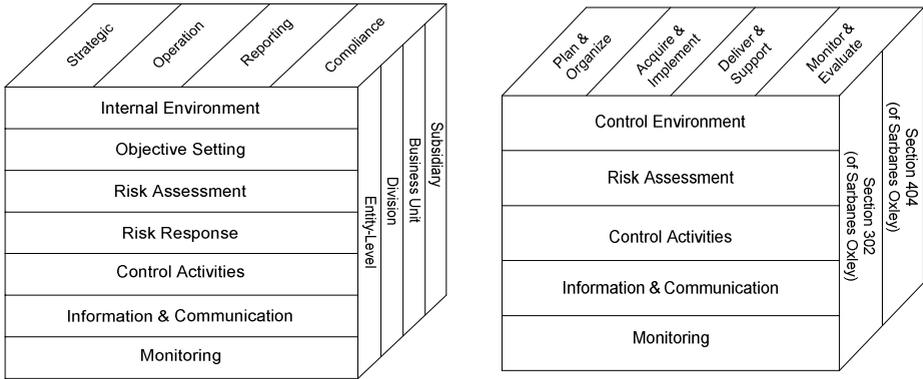
Fig. 3. COSO Enterprise Risk Management Framework (left) and CobIT (right)

COSO's ERM has been broadly adopted by businesses since the Sarbanes-Oxley Act was ratified 2002. The act requests businesses to assure the quality of financial reports as well as the existence and adherence to internal control policies.

The Control Objectives for Information and related Technologies (CobIT) created by the IT Governance Institute (ITGI) is a set of audit-oriented guidelines that helps businesses improve their IT governance [19]. ITGI believes that effective management of information and related technology infrastructure will improve business performance. In addition to the effective and efficient delivery of information, IT governance is charged with realizing risk management by improving information security, accountability, and integrity. The CobIT Framework consists of four high level control objectives: Planning and Organization, Acquisition and Implementation, Delivery and Support, and Monitoring. With regard to the individual components within these objectives, ITGI has adopted the COSO ERM framework. However, only five of the original eight components are applied by ITGI: Control environment, risk assessment, control activities, information and communication, and monitoring. The COSO framework is based on the assumption that during the implementation of CobIT control objectives, business entities will be able to identify risks that endanger the usage of information throughout the organization and further mitigate these threats before they result in financial or organizational damages.

Both COSO ERM and CobIT are useful frameworks that can guide the actions of a BPM project manager to structure risk recognition and mitigation activities. While the ERM framework is more comprehensive in the sense that it lists individual risk areas in more detail, the CobIT framework is more closely aligned with the lifecycle concept that guides most BPM efforts.

6   Summary and Outlook

In this paper we have discussed risks that are part of the Business Process Management Lifecycle. Based on an analysis of risk taxonomies in the academic literature we have classified risk factors that can be associated with the individual phases of the BPM lifecycle. The majority of risk factors identified relate to the

composition of a BPM project: The selection of stakeholders, mismatches between design and implementation methods, and the mismatch of organizational, process, implementation, and evaluation goals and metrics. By mapping the lifecycle risks to a functional framework we have shown that some risks are specific to individual lifecycle phases, while system, leadership, resource, and strategy-related risks affect the BPM lifecycle in its entirety. Our study shows that BPM projects are faced with risks both within individual lifecycle phases, as well as with risks during the transition between lifecycle phases. While we did not elaborate on practical risk mitigation strategies for BPM projects in this paper, our future work focuses on the mapping of these risks to activities within the COSO and CobIT frameworks. This continued effort will hopefully lead to practical risk mitigation strategies for BPM projects.

References

[1] Grover, V.: From Business Reengineering to Business Process Change Management: A Longitudinal Study of Trends and Practices. IEEE Transactions on Engineering Management 46 (1999) 36-46

[2] Clemons, E. K., Thatcher, M. E., Row, M. C.: Identifying Sources of Reengineering Failures: A Study of the Behavioral Factors Contributing to Reengineering Risks. Journal of Management Information Systems 12 (1995) 9 - 36

[3] Kliem, R. L.: Risk Management for Business Process Reengineering Projects. Information Systems Management 17 (2000) 71-73

[4] Smith, H., Fingar, P.: Business Process Management - The Third Wave. Meghan Kiffer Press, Tampa, FL (2003)

[5] Zairi, M., Sinclair, D.: Business Process re-engineering and process management. Business Process Re-engineering & Management Journal 1 (1995) 8 - 30

[6] Elzinga, D. J., Horak, T., Lee, C.-Y., Bruner, C.: Business Process Management: Survey and Methodology. IEEE Transactions on Engineering Management 42 (1995) 119 - 128

[7] Harmon, P.: Evaluating an Organization's Business Process Maturity. Business Process Trends 2 (2004)

[8] March, J. G., Shapira, Z.: Managerial Perspectives on Risk and Risk Taking. Management Science 33 (1987) 1404-1418

[9] Wiegers, K.: Knowing your enemy: software risk management. Software Development 6 (1998)

[10] Charette, R.: Applications Strategies for Risk Management. McGraw-Hill, New York (1990)

[11] COSO: Enterprise Risk Management - Integrated Framework. Executive Summary. Committee of Sponsoring Organizations of the Threadway Commission, (2004)

[12] Gemmer, A.: Risk management: moving beyond process. Computer 30 (1997) 33 - 43

[13] Adler, T. R., Leonard, J. G., Nordgren, R. K.: Improving Risk Management: Moving from Risk elimination to Risk Avoidance. Information and Software Technology 41 (1999) 29-34

[14] Peltier, T. R.: Risk Analysis and Risk Management. The EDP Audit, Control, and Security Newsletter 32 (2004)

[15] Davenport, T. H.: Process Innovation. Harvard Business School Press, Boston, Massachusetts (1993)

[16] Scott, J. E., Vessey, I.: Managing Risks in Enterprise Systems Implementations. Communications of the ACM 45 (2000) 74-81

[17] Sumner, M.: Risk Factors in Enterprise-wide/ERP projects. Journal of Information Technology 15 (2000) 317-327

[18] Somers, T. M., Nelson, K. G.: A Taxonomy of Players and Activities across the ERP Project Life Cycle. Information and Management 41 (2002) 257 - 278

[19] IT Governance Institute (ITGI): IT Control objectives for Sarbanes-Oxley. http://www.itgi.org/template_ITGI.cfm?template=/ContentManagement/ContentDisplay.cfm&ContentID=14133

[20] Jaafari, A.: Management of Risks, Uncertainties and Opportunities on Projects: Time for a Fundamental Shift. International Journal of Project Management 19-2 (February 2001) 89-101.

[21] Miller, R., and Lessard, D.: Understanding and Managing Risks in Large Engineering Projects. International Journal of Project Management 19 (2001) 437-443

[22] Ward, S., and Chapman, C.: Transforming Project Risk Management into Project Uncertainty Management. International Journal of Project Management 21-2 (1994) 97-105

[23] Project Management Institute: A Guide to the Project Management Body of Knowledge (PMBOK Guide), 2000 edition. Project Management Institute

[24] Levin, H.S.: Office Work and Automation. John Wiley & Sons, New York 1956.

[25] zur Muehlen, M.; Rosemann, M.: Integrating Risks in Business Process Models. In: Proceedings of the 2005 Australasian Conference on Information Systems (ACIS 2005), Manly, Sydney, Australia, November 30-December 2, 2005.