

# Risk Management in the BPM Lifecycle

Michael zur Muehlen, 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 (BPM) is considered an essential strategy to create and maintain sustainable competitive advantage. While researchers are anxious to identify critical success factors for the management of business process related projects, the risks associated with these projects have received considerably less attention. This is a concern: Although BPM projects contain phases that relate to software development and deployment, simply applying 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 the individual life cycle phases and transitions we discuss four strategies to deal with these risks: avoid, mitigate, transfer, and accept. The outlook of this paper discusses how assessment frameworks such as CobIT and COSO relate to the identified risks.

## Motivation

Business Process Management entails a 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 or services tend to remain a core binding element for organizations. Consequently, structuring organizations around business processes is a popular topic in both the management and technical literature. A study conducted by Grover indicates that, even with enormous time and investment devoted, 7 out of 10 business process projects failed in the past [1]. Such high failure rate implies that in addition to understanding what has to be done in process reengineering projects, what should *not* be done deserves equal attention. We are particularly interested in the risks that endanger the success of business process projects, such as those described in [2, 3].

In this paper, we describe the risks that BPM projects are exposed to along the BPM lifecycle. Based on four risk management strategies we discuss the options 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.

## Business Process Management

While the general notion of process is widely understood, a variety of authors has provided different definitions for the term process. We see a process as a sequence of activities that are necessary to manipulate an economically relevant object towards a specific goal. Business processes can be described at different levels of abstraction. Typically they are seen as high level processes determined by the overall goals of the enterprise that contain interfaces to market partners (i.e., customers, suppliers, or third parties).

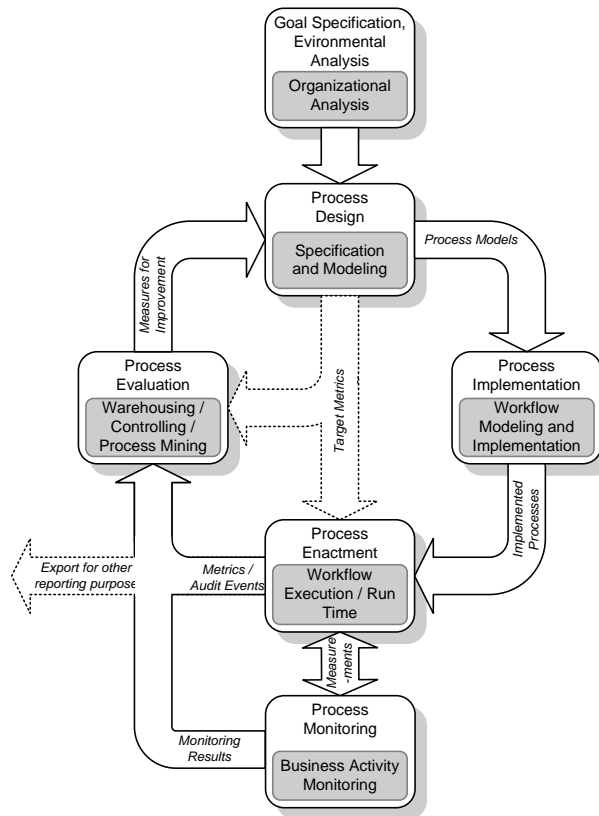
Management in general is a cross-sectional function that controls the use of resources and choreographs the operational activities of the enterprise. Management functions follow a lifecycle of planning, organizing, staffing, directing and controlling, and budgeting. Business Process Management is the 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 clearly not new.

Zairi and Sinclair state that BPM is "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. Thus, 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 [7]: "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."

The core task of Business Process Management is 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.

The purpose of the process design phase is the identification of those processes an organization wishes to analyze, (re-)design, 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 processes, and the affected organization. External variables reflect the influence of outside players such as suppliers, customers, competitors, or governmental agencies. The completeness of the goal specification and the organizational analysis defines the parameters and thus the constraints for the process (re-)design.



**Fig. 1.** Business Process Management Lifecycle

During the process implementation phase the specified processes are transferred into operational environments which can either be manual (e.g. via procedure handbooks) or automated (e.g. via BPM or workflow software). Finally, process are executed and monitored in real time. For the purpose of process control, audit trails produced from process enactment and monitoring stages can be used in the evaluation stage. Feedbacks and contingency plans for process improvement can be formulated based on the results of process measurement and evaluation.

### 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].

The purpose of risk management is to “reduce or neutralize potential [risks], and simultaneously 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]. Risks are caused by various of uncertainties [12], hence it is not easy to frame risks in a precise fashion. One way to do so is to have risks characterized 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 the strategies in detail.

<b>RISK MGMT. STRATEGY</b>	<b>DEFINITION</b>	<b>EXAMPLES</b>
<b>Mitigation</b>	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.	<ul style="list-style-type: none"> <li>• Standardized process routing</li> <li>• Formalized exception handling</li> <li>• Complete kit processing</li> <li>• Collaboration, checks &amp; balances</li> </ul>
<b>Avoidance</b>	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.	<ul style="list-style-type: none"> <li>• Process redesign</li> </ul>
<b>Transfer</b>	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.	<ul style="list-style-type: none"> <li>• Process Outsourcing</li> <li>• Insurance Policies</li> </ul>
<b>Acceptance/ Assumption</b>	To adapt to the risk when it becomes a problem. The enactment of a risk contingency plan is required in this strategy.	<ul style="list-style-type: none"> <li>• Adaptation to regulatory requirements</li> </ul>

**Table 1.** Risk Management Strategies

### **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]. 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].

### 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). BPM project managers need to pay particular attention to these areas.

PHASE	BPM RISK
[analysis]	<ul style="list-style-type: none"> <li>• Conduct analysis without a strategic view</li> <li>• Failure to define process goals/values in a language understandable for process stakeholders</li> <li>• Overemphasis of technical variables</li> <li>• Failure to relate systematic/organizational risks to the analysis</li> </ul>
[analysis to design]	<ul style="list-style-type: none"> <li>• Method failure in mapping analysis outcomes to process models</li> <li>• Loss of information during the mapping processes</li> </ul>
[design]	<ul style="list-style-type: none"> <li>• Implementation modeling languages are not capable to construct designated functionalities of the process</li> <li>• Implementation of multiple modeling technologies</li> <li>• Lack/absence of conversation between process designers and process stakeholders</li> <li>• Designers ignore the organizational perspective of design</li> <li>• Risk handling mechanisms are missing in the design</li> </ul>
[design to implementation]	<ul style="list-style-type: none"> <li>• Wrong translation from process models to implementation plans</li> <li>• Mismatch of design method and implementation method/perspective</li> </ul>
[implementation]	<ul style="list-style-type: none"> <li>• Lack of a high level view of the implementation (for executives)</li> <li>• Management level lacks adequate knowledge of process management</li> <li>• Overemphasis on technical issues</li> <li>• Designed models are not applicable to the current infrastructure</li> <li>• Designed models are not applicable to the current organizational structure</li> <li>• Failure to relocate the resources</li> <li>• Failure to rearrange/reassign roles and responsibilities to process stakeholders</li> <li>• Process stakeholders assume they know the new processes and their roles without review of the redesign</li> </ul>

[execution]	<ul style="list-style-type: none"> <li>• Resistance from stakeholders to perform process-oriented activities</li> <li>• Stakeholders feel uncomfortable under process-oriented leadership</li> <li>• Stakeholders take too long to adapt to process-oriented work style</li> <li>• Stakeholders are unable to perform collaboration across divisions</li> <li>• Lack of conversation and a common language among stakeholders</li> <li>• The composition of stakeholders changes during the runtime</li> <li>• System instability in the runtime environment</li> <li>• Service vendors merge or go out of business</li> <li>• New regulatory requirements make current process practices illegal</li> </ul>
[monitoring]	<ul style="list-style-type: none"> <li>• Lack of monitoring strategies, plans, objectives, and methods</li> <li>• Stakeholders/Laws prohibit process transparency (monitoring)</li> <li>• Flawed information produced by stakeholders</li> <li>• Absence of a precise information filtering policies</li> <li>• Monitoring without a qualitative perspective (i.e. numerical focus)</li> <li>• Monitored objectives are different from design objectives</li> </ul>
[monitoring and execution to controlling]	<ul style="list-style-type: none"> <li>• Information overload of monitoring recipients</li> <li>• Failure to translate raw audit data into useful information</li> <li>• Lack of management in merging multiple information channels</li> <li>• Intraceable human interference in the process</li> <li>• Failure to report critical issues to allow timely response</li> </ul>
[controlling]	<ul style="list-style-type: none"> <li>• Standards for evaluation policies/methods are missing</li> <li>• Controlling objectives are different from process design objectives</li> <li>• Misinterpretation of audit data</li> <li>• Missing link from audit data to business data</li> <li>• Failure to relate the evaluation to strategic and external variables</li> </ul>
[controlling to design]	<ul style="list-style-type: none"> <li>• Lack of well-defined feedback mechanisms</li> <li>• Inability to recognize problems from the evaluation</li> <li>• Failure to derive contingency plans from the evaluation</li> <li>• Controlling and process improvement conducted by different stakeholders</li> </ul>

**Table 3.** Examples for BPM-specific Risks

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

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

**Table 4.** Risk Classification

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 life cycle 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].

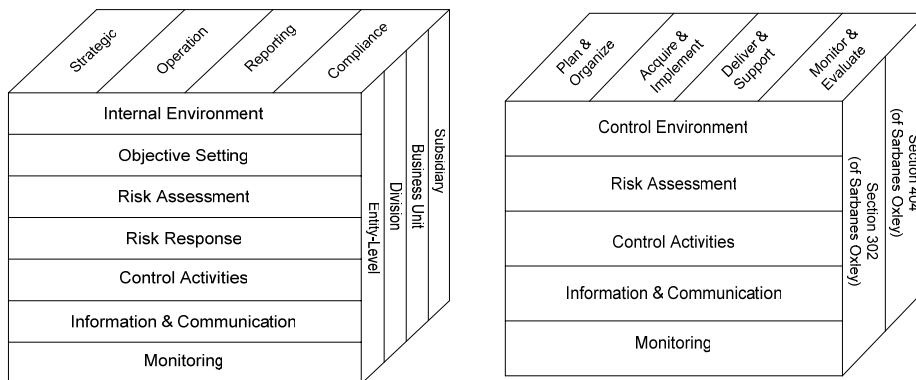
RISK FACTOR	LIFE CYCLE RISKS BREAKDOWN
<b>Method</b>	<ul style="list-style-type: none"> <li>• Invalid process analysis/design methods [1], [2]</li> <li>• Invalid mapping methods (problem to solution, solution to implementation) [1, 2], [2, 3]</li> <li>• Invalid process modeling methods [2, 3]</li> <li>• Invalid process implementation methods [3]</li> <li>• Invalid evaluation methods [5]</li> <li>• Inconsistency of evaluation/measurement methods [5], [6]</li> <li>• Invalid feedback mechanism [5, 2]</li> </ul>
<b>Communication</b>	<ul style="list-style-type: none"> <li>• Miscommunication of goals [ALL]</li> <li>• Lack of communication between stakeholders [ALL]</li> </ul>
<b>Information</b>	<ul style="list-style-type: none"> <li>• Misusage of information [1,2], [4,6], [5]</li> <li>• Inadequate information [ALL]</li> <li>• Invalid information [1, 2], [2, 3], [5, 2]</li> <li>• Invalid information conversion [6, 5]</li> </ul>
<b>System / Technology</b>	<ul style="list-style-type: none"> <li>• Lacking technology acceptance [ALL]</li> <li>• Misusage of technology [ALL]</li> <li>• Lack of technology flexibility [ALL]</li> <li>• Lack of technology compatibility [ALL]</li> <li>• Lack of technology scalability [ALL]</li> </ul>
<b>Leadership / Management</b>	<ul style="list-style-type: none"> <li>• Lack of leadership/management [ALL]</li> <li>• Inconsistency of leadership/management [ALL]</li> <li>• Absence of leadership/management [ALL]</li> </ul>
<b>Resource / Skill</b>	<ul style="list-style-type: none"> <li>• Absence of resource/skill [ALL]</li> <li>• Misusage of resource/skill [ALL]</li> <li>• Inability to use resource/skill [ALL]</li> </ul>
<b>Adaptation to Change</b>	<ul style="list-style-type: none"> <li>• Failure to redesign jobs/functions [1, 2]</li> <li>• Failure to perform necessary changes [2]</li> <li>• Inability to recognize problems [5, 2]</li> <li>• Inability to react to designated changes [ALL]</li> </ul>
<b>Strategic Thinking</b>	<ul style="list-style-type: none"> <li>• Inaccurate strategic definition [ALL]</li> <li>• Unclear strategic definition [ALL]</li> <li>• Absence of strategic definition [ALL]</li> </ul>

Table 5. Mapping of BPM Risk to Risk Classification.

### 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 life cycle that should include the following key concepts: analysis, design, construction, test, and maintenance [14]. In either case, there exists a consensus that a life cycle 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” means all the policies and procedures adopted to assist in achieving management’s objective of ensuring the orderly and efficient conduct of its 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 impacts produced by risks, there are 4 major objectives where risk management must be delivered: strategy, operations, reporting, and compliance. In addition, in dealing with each of the objectives, 8 components have to be taken into account. They are the internal environment, objective setting, event identification, risk assessment, risk response, control activities, information and communication, and monitoring. COSO’s ERM has been broadly adopted by business entities since the Sarbanes-Oxley Act was ratified 2002. The act requests businesses to assurance the quality of financial reports as well as business internal control policies. The high adoption of ERM suggests the significant of business compliance with law enforcement and regulation risks.



**Figure 2.** COSO Enterprise Risk Management Framework (left) and CobIT (right)

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 in information and related IT will produce symmetric success in business performance. In addition to effective and efficient information delivery, realizing risk management by improving information security, accountability, and integrity have become one of the biggest challenges in IT governance. ITGI presents 4 high level IT control objectives: planning & organization, acquisition & implementation, delivery & support, monitoring. Regarding the components, ITGI adopts the ERM framework by COSO and simplifies it into 5 IT management components: control environment, risk assessment, control activities, information & communication, and monitoring. It suggests that during the cycle of delivering CobIT

control objectives, business entities will be able to identify risks that endanger the usage of information throughout the organization and further mitigate their threats before the crisis are caused.

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 life-cycle concept found in the general notion of BPM efforts.

## Summary and Outlook

In this paper we have discussed risks that are part of the Business Process Management Lifecycle. Based on literature-based risk taxonomies we classified examples of management risk that can be associated with the individual phases of the BPM life cycle. The majority of risk factors identified relate to the composition of BPM project stakeholders, mismatches between methods, and the mismatch of organizational, process, implementation, and evaluation goals and metrics. Our study shows that BPM projects are faced with risks both within individual life cycle phases, as well as in the transition between life cycle 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, which 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](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