



COVER SHEET

Rikhardsson, Pall and Best, Peter J and Green, Peter and Rosemann, Michael (2006) Business Process Risk Management and Internal Control: A proposed Research Agenda in the context of Compliance and ERP systems. In *Proceedings Second Asia/Pacific Research Symposium on Accounting Information Systems*, Melbourne.

Accessed from <http://eprints.qut.edu.au>

Copyright 2006 the authors

Business Process Risk Management, Compliance and Internal Control: A Research Agenda*

Pall Rikhardsson (corresponding author)
Department of Business Studies
The Aarhus School of Business
Fuglesangs Alle 4
8210 Aarhus V
Denmark

Telephone: (+45) 89486688
Telephone (direct): (+45) 89486376
Fax: (+45) 86151290
Mobile: (+45) 22285598
E-mail: par@asb.dk

Peter Best
Faculty of Business, Queensland University of Technology

Peter Green
The University of Queensland Business School, The University of Queensland

Michael Rosemann
Faculty of Information Technology, Queensland University of Technology

Abstract

Integration of risk management and management control is emerging as an important area in the wake of the Sarbanes-Oxley Act and with ongoing development of frameworks such as the Enterprise Risk Management (ERM) framework from the Committee of Sponsoring Organizations of the Treadway Commission (COSO). Based on an inductive methodological approach using literature review and interviews with managers engaged in risk management and internal control projects, this paper identifies three main areas that currently have management attention. These are business process risk management, compliance management and internal control development. This paper discusses these issues and identifies a series of research questions regarding these critical issues.

Keywords

Risk Management, Internal control, Business processes, Compliance, Sarbanes-Oxley Act, ERP systems, COSO, COBIT

* This is research in progress. Not to be quoted.

1. Introduction

We live in an unsure world. Things we thought could never happen have happened and things we thought would happen did not. In the aftermath of extensive financial collapses, terrorist attacks, failure of large computer systems and health scares, there is increased focus on risk management - not only as a specific aspect of company operations but as an integrated organisational issue spanning corporate and geographical boundaries.

Risk management is a relatively mature research area in various operating functions such as production, logistics, information technology, and health and safety (Charette 1990; Borodzicz 2005). Decision making theory defines risk as "reflecting variation in the distribution of possible outcomes, their likelihoods, and their subjective values" (March & Saphira 1987). Risk can be expressed mathematically as "the probability of occurrence of loss/gain multiplied by its respective magnitude" (Jaafari 2001).

Risk assessment involves identifying threats and assessing the probability of these threats actually occurring. *Risk management* is about managing what should happen if these threats materialise including disaster recovery plans, crisis management and emergency procedures (Borodzicz 2005). It is also about minimizing the probability of the threat leading to undesired effects by designing, implementing and operating *internal controls* that mitigate, avoid or transfer risk (Ibid).

Perhaps, the most widely acknowledged definition of internal controls is from The Committee of Sponsoring Organizations of the Treadway Commission (COSO) (COSO 1992; 2004) which defines it as a process, effected by an entity's board of directors, management and other personnel, designed to provide reasonable assurance regarding the achievement of objectives regarding: (i) company strategy; (ii) effectiveness and efficiency of operations; (iii) reliability of financial reporting; and (iv) compliance with applicable laws and regulations.

This paper reports on the results of a research project focusing on the links between risk management and internal controls. As this is an emerging research field this paper aims to develop a practice-driven understanding of the concepts and issues involved. Based on interviews with practitioners and a subsequent literature review it proposes a research agenda that can guide interested researchers in this fast developing domain.

The structure of the paper is as follows. The next section describes the methodology of the project, section 3 presents the results, section 4 discusses these results and section 5 concludes the paper with a proposed research agenda.

2. Methodology

Based on an inductive research approach, the goal of this project was to clarify the issues involved and to propose a practice-driven research agenda. For this purpose a two step approach was chosen:

1. Initial exploratory interviews with selected practitioners with the aim of clarifying the link between risk management and internal control as well as identifying important issues.
2. Subsequent literature review to assess what current research has to offer regarding the issues identified during the interviews. The literature review focused on both academic journals as well as practitioner-oriented publications. The latter were included as emerging issues which often first appear in these types of journals.

The interviews were scheduled with five large international companies. Three of the meetings were personal meetings while two of the meetings were telephone conferences. The selection of these companies was mainly based on:

1. Issue awareness: The companies had to have focus on risk management and internal controls. This focus could be either as a part of their operations or as a service (i.e. consultancies).
2. Size: The companies had to be of a size sufficient for risk management and internal controls to be formalized processes.
3. Accessibility: The companies selected were based on prior evidence of their support for research projects and their links with the involved research institutions.

The characteristics of the companies interviewed are shown in table 1.

| | Company 1 | Company 2 | Company 3 | Company 4 | Company 5 |
|--------------------------------------|---------------------------------------|--------------------------|------------------------------|--------------------------|--------------------------|
| Industry | Bank | Bank | Mining | Auditing/ consultancy | Auditing/ consultancy |
| Turnover 2005 (worldwide) | AUD 13,8 billion | AUD 11,3 billion | AUD 21,0 billion | AUD 29,3 billion | AUD 21,8 billion |
| Full time employees 2005 (worldwide) | 39,000 | 35,000 | 33,000 | 130,000 | 120,000 |
| Manager interviewed | Manager Quality & Business Efficiency | Manager Operational Risk | Business Improvement Manager | Senior manager | Senior manager |

Table 1: The companies interviewed.

An exploratory interview methodology was adopted employing a semi-structured interview guide listing several broad issues within risk management and internal controls. However, these were used in a very loose manner encouraging the managers to speak of what currently had their attention regarding risk management and internal controls.

We realise of course the empirical limitations of our approach. The purpose of the sample is to point out areas that currently have management attention and thereby act as a focus for the literature search.

3. Results

In the interviews with the five managers, the issues discussed could be classified within three broad areas emerged based on descriptions of either “projects in progress” in the companies or based on issues that had management attention. These are:

1. Business process risk management
2. Compliance
3. Developing internal control

These are described below describing the issues identified in the interviews followed by the results from the literature review.

Business Process Risk management: The Interviews.

Linking business process management and business process modelling to risk management seemed to have a great deal of interest. The managers described several issues within this field:

1. The managers mentioned differences in risk perception both at an organizational level and at process level. The implications of these for the management of business process risk are unclear though. Furthermore, management conceptualization of risk in business processes (e.g. operational risk, IT risk, financial risk, compliance risk, legal risk, health and safety risk etc.) differs between functions and organisations which could impact the management of these processes.
2. Risk needs to be described in a consistent manner across various levels of business process architectures. Currently there is no one method or modelling tool used for this purpose. A method for mapping and describing risk needs to be integrated with business process modelling languages.
3. As companies are becoming more global in their operations, with their organization more distributed and linkages into global supply chains, the level of risk evaluation and management is changing. There is a shift in focus from local and regional risks to global risks. Understanding the impact of this shift on business processes is crucial.
4. The materialization of risk and the resulting effects cost money but so do risk management and control, both directly but also as a potential loss of effectiveness and opportunity. The managers referred to the importance of understanding the costs of risks and the costs of mitigating these risks in a business process perspective including the costs of letting the risk materialize versus the costs of controlling for that risk.

Business process risk management: The Literature

Business process management has been identified as one of key issues in business management (Harmon 2003) The term Business Process Management (or BPM) refers to a set of activities which organizations can perform to either optimize their business processes or adapt them to new organizational needs. Business processes of the organization can be seen as the place where risk materializes, where information is generated and used and where control activities are carried out.

There is a tight relationship between business processes and risks. On the one side, risk management can be seen as a business process, i.e. the different stages of the risk life-cycle form a business process, which requires management. On the other

side, risk is an important business phenomenon, which increasingly has to be considered in the (re-)design of business processes. Though there is such a close link, the process and risk management communities are rather separate groups with different research agendas and methodologies (zur Muellen & Rosemann 2005).

The purpose of risk management is to “reduce or neutralize potential [risks], and simultaneously offer opportunities for positive improvement in performance.” (Ward & Chapmann 1994, p. 23). A general risk management framework is composed of three main action phases: identification, analysis and control (Kliem 2000). Risks are caused by various uncertainties. Hence it is not easy to frame risks in a precise fashion. One way to do so is to have risks characterised using properties such as impact, probability, time frame and coupling with other risks (Gemmer 1997). Since risks are commonly associated with negative outcomes (March et al. 1987), the distinction between risks and problems often remains unclear. Risk is not necessarily a problem, but a “potential problem” that may result from making a particular decision (Charette 1990).

In the context of process management, risk has mainly been addressed as a factor in the management of process-related projects. A notable exception is the case study by Ballou (et al. 2000). The authors discuss risk at the business process level, but their study of the processes remains at a high level of abstraction and risk is only dealt with from a financial and general business risk perspective, while operational risk at the task level is not addressed.

Suh and Han (2003) propose the use of functional decomposition and the Analytic Hierarchy Process to identify business related risks in the information system (IS) infrastructure of an organisation. They use a functional model of business operations as a guideline to evaluate the criticality of individual IS components. This traditional view of the organisation does not account for cross-functional components that may support multiple business functions and does not support a process-oriented view of business operations.

Yu et al. (1999) discusses different models to assess possible failure modes, effects and their criticality. It lists the risk priority number method and the expected cost method as suitable to determine process-related risks. Based on manual operating procedures the authors then present a human error criticality analysis technique that allows for the valuation of possible human error in a given business process. This analysis technique leads to an error tree with probabilities, but does not integrate with other conceptual modelling techniques.

An influential control framework that linking risk management to business processes as well as internal control is the COBIT framework. Particularly in the the latest version of the framework (COBIT 4.0 in ITGI 2005) and in the specific application of the framework to Sarbanes-Oxley compliance (ITGI 2004). The COBIT framework for managing compliance risk and control specifically focuses on general, company-wide and application controls that are related to business processes such as manufacturing, sales and logistics.

The above clearly indicates a demand for more conceptual guidance in relation to risk-aware process management principles. There is a need to integrate risk as an artefact in established enterprise architectures and business modelling techniques

and tools. Furthermore, there is the requirement to develop technical risk architectures - i.e. the integration of all risk management systems into one holistic solution. This has not been addressed in the literature as of yet.

Compliance management: The Interviews

Another area that currently holds management attention is compliance. Although spurred by high-profile legislation like the Sarbanes-Oxley Act, compliance is a broad area and includes compliance with health and safety laws and regulations, environmental laws and regulations, labour laws and consumer protection legislation. However, the managers interviewed saw these in a risk management perspective with focus on the risk of non-compliance and were concerned with the organization and controls necessary to ensure compliance. Issues mentioned were:

1. Compliance is a business process and could be approached as such. However, approaching compliance in this manner is still in its infancy and differences in and integration of different compliance processes across the organization (at local, regional and global levels) are not yet well understood. Neither is there any general way of modelling and describing the compliance management process and its links to business process models.
2. In particular, the managers mentioned some compliance issues as being global. For example, for a parent company operating in the US, the Sarbanes-Oxley requirements will impact on all of its controlled entities. Another example is a company that chooses to operate its facilities around the world according to some best practice environmental standard to which its entities have to comply. Global compliance further complicates the issues inherent in local compliance processes and adds some new challenges.
3. Not complying with legislation can cost money in fines. However, it can also cost money due to damage to the reputation to the company, loss of consumer trust or loss of investor interest. Measuring these costs can be important regarding e.g. decisions whether to operate in a region or not.
4. Compliance management goes through a life cycle like most other management processes. There is however, no clear understanding of the phases compliance management goes through, such as no integration to full integration in business processes, manual to automated, local to global, disaggregated organizational responsibility to a chief compliance manager and so on. The accountability structure for compliance was mentioned as important, as increased focus on compliance (as more complex compliance structures imply) increases the need for a coordination and managing function in the company.

Compliance management: The Literature

It seems that in the past couple of years, compliance has become something of a buzzword. However, companies have always had to comply with laws and regulations including health and safety requirements, tax laws, consumer protection laws and labour laws.

Factors that have increased the current focus on compliance management are:

1. Extensive emerging compliance requirements (such as Sarbanes-Oxley (SOX) compliance) requiring compliance on local, regional and global levels

across different business processes and in some cases attestation by highest levels of management

2. Rising costs of compliance. A study of Fortune 1000 by Charles Rivers & Assoc. in 2005 showed that companies spent on average US\$ 5.9 million on compliance with SOX requirements in 2004 (CRA 2005). A similar study by AMR Research concludes that compliance costs are expected to rise significantly in 2005-2010 (IMJ, 2004). As costs rise, managers look for ways to increase the efficiency and effectiveness of compliance processes
3. Non-compliance costs time and resources including indirect costs such as reputation damage costs and costs of defending lawsuits. Specifically, the risks of reputation damage are important to those companies that depend on public trust or sell high profile products to end consumers (Testa 2005, DrugResearcher 2004)
4. Integration of business processes, information technology and people across geographical, temporal and organizational boundaries is leading to new types of compliance risks that have to be addressed. An example could be varying local hazardous product transport regulations that have to be complied with across a global supply chain.

These developments call for increased management of compliance and even for making it the responsibility of a specific management function (i.e. chief compliance officer). It also can lead to the development or acquisition of a specific compliance management information system.

The passing of the SOX legislation in the US has had significant influence on how companies see compliance (Baker et al. 2006). The fundamental aim of SOX is to minimize the risk of fraud and significantly misrepresented financial statements. Companies have to focus explicitly on different types of risks (such as the risk of false information in annual reports or misappropriation of funds) and the internal controls that address these risks. High level managers then have to publicly attest to the reliability of these controls. This situation adds an external compliance dimension to the concept of risk management and control (ITGI 2004; COSO 2004; CFO 2005).

Compliance risk management has been addressed within separate compliance areas such as SOX, internal controls and reporting (e.g. Waldman 2005; Shue 2004; Kendal 2004; Byington & Christensen 2005), environmental compliance (Gangadharan 2006), occupational health and safety (Ashford & Caldart 2001) and various labour laws including discrimination laws, child labour and employee protection (Adams 2003).

Compliance is a general feature of business. First of all every company has to comply with some legislation. Secondly, it is a process composed of different stages such as overview of legislation, identification of requirements, evaluation of practice, assessment of non-compliance risks, assignment of accountability, project management, reporting structures, etc. However, there seems not to be any research focus on integrating compliance processes across functions, developing standardised compliance processes or exploring compliance issues in a regional or global context or how to manage and improve compliance in a business process perspective.

Internal control development: The Interviews

The third area is internal controls and how these are developed and integrated in both risk management and compliance. These are mentioned as even more important in recent years. Issues identified were:

1. Internal controls have always been a part of the management process focusing on implementing strategy and achieving objectives. Recently internal controls have emerged as key issues in risk management and compliance management. Controls are in place to mitigate risk, some of which are inherent in business processes (i.e. the risk of fraud, the risk of data errors etc.) and to secure compliance with legislation or with management objectives. The integration between business processes, risk management and controls is not advanced as of yet and is often "learning by doing" in companies.
2. The requirements of Sarbanes-Oxley necessitate substantial improvements in internal controls. Over time internal controls seem to go through several stages of development. This development, the characteristics of each stage, and contingency factors affecting each stage, are not well understood but are important as companies could improve their performance by having an overview of strengths and weaknesses at each stage.
3. Internal controls operate on many levels. There are e.g. behavioural controls, information controls, operational controls, preventive controls, detective controls, application controls and general controls. Internal controls however are dependent on the control environment. Control environment factors include the integrity, ethical values and competence of the entity's people, management's philosophy and operating style, the way management assigns authority and responsibility, how the entity organizes and develops its people, and the attention and direction provided by the board of directors. However, the relationship between these general organization wide controls and individual control activities are not well understood.
4. Specific issues surrounding Sarbanes-Oxley compliance were raised by the auditing managers interviewed. They would like to know more about companies' and auditing firm's interpretations of materiality, material weaknesses, significant deficiencies and effectiveness of controls in a SOX context. Furthermore, understanding disclosures of internal control weaknesses in corporate annual reports emerged as an issue.

It seems that the managers interviewed see these three areas as closely interrelated. That is to say compliance efforts, risk management in business processes and the development of internal controls are linked to certain activities. Examples mentioned were Sarbanes-Oxley which is a compliance effort that requires risk assessments and development of internal controls. Another example mentioned is disposal of nuclear waste which requires extensive risk management procedures, has to comply with legislation and is dependent on numerous internal control procedures. A third example is fraud detection which requires risk assessment, development of internal controls and affects compliance with financial reporting legislation.

Internal control development: The Literature

A review of the literature raises the following question: Is there a difference between internal control and management control? There are different definitions (Rikhardsson et al. 2005) but these two concepts are closely linked. Both focus on

the ability of managers to steer the organisations in the direction specified by organisational strategy and objectives as well as identifying and reacting to internal and external changes that might affect this course. An often-used definition of management control is "... the formal, information based routines and procedures managers use to maintain or alter patterns in organizational activities" (Simons 1995: p. 5). However, the internal control definition by COSO (1992) also includes compliance and external reporting as specific control objectives as well as strategy and operations. Thus it would seem that internal controls as a concept is more specific than the more academic definition of management control.

The review of the relevant literature shows that the evolution of academic understanding of management control and internal control has gone through at least two evolutionary phases in the last decades. These phases are to be seen as complementary and not as resulting in mutually exclusive understanding of internal control.

From the 1960s and onwards management control is seen as a cybernetic management system including environmental impulses, organizational responses and achievement of organizational objectives. Management control is seen mainly as an information process where managers plan, act and react to internal and external impulses (e.g. Ittner & Larcker 2001; Otley & Berry 1980; Flamholtz et al. 1985). In the 1990s the view starts to emerge that management control is a system or a process focused on implementing strategy in an environment where strategy needs to be revised on an ongoing basis (e.g. Simons, 1995; 2000; Kaplan and Norton 1996, Chenhall 2003; Anthony & Govindarajan 2003; Merchant & Van der Stede 2003).

A review of the more recent literature, however, suggests that the academic and practitioner understanding of management control is entering a third phase where the focus is on the more specific concept of internal control. This sees internal control as a system aimed at assessing, minimizing and controlling risk associated with company business processes, business transactions, information technology applications and information dissemination to internal and external decision makers (e.g. ITGI 2004; COSO 2004; zur Muehlen & Rosemann 2005; Rikhardsson et al. 2005).

This focus on risk and risk management in internal control is apparent in some influential frameworks that recently have been published within the field. One such framework is the COSO Enterprise Risk Management (ERM) framework (from 2004 but building in an earlier framework by COSO from 1992).

In COSO's Enterprise Risk Management (ERM) framework, enterprise risk management is defined as follows (COSO 2004, p. 2): "Enterprise risk management is 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 regarding the achievement of entity objectives".

Apart from previous frameworks and tools developed in the past two evolutionary stages, currently internal control frameworks and tools are emerging that link risk management to internal controls. These can be classified into general frameworks

such as COSOs ERM framework (COSO 2004) and specific frameworks or studies tailored to various contexts including information technology (Shue 2004; Cannon & Grove 2004; Hamaker & Hutton 2004; CFO 2005), corporate compliance (CRA 2005, Stephens 2005; Markham & Hamerman 2005; Byington & Christensen 2005; Waldman 2005; Matyjewicz & D'Arcangelo 2004) and business process management and modelling (Zur Muellen & Rosemann 2005).

There is thus emerging research into the links between risk management and internal control. However, to a large extent, there seems to be focus on developing frameworks and interpreting institutional developments. There is a need for large scale surveys documenting company similarities and differences, what influences internal control development in which settings as well as industry characteristics. There is also a need for case studies documenting company practice and experiences with the aim of further developing practice.

4. Discussion

Generally, few academic studies have focused explicitly on the integration of risk management, compliance and internal control. Practitioner journals (such as *Accountancy*, *Internal Auditor* and *The Information System and Control Journal*) have concentrated on these issues for some time though.

The literature review shows that business process risk and internal control are being integrated in several frameworks such as the Enterprise Risk Management model from COSO (2004) and the COBIT from ITGI (2005). The integration of compliance, internal controls and risk assessment is addressed in the application of the COBIT framework to SOX compliance in ITGI (2004).

In these frameworks, internal controls can be seen as focusing on two aspects:

1. Controlling *behaviour* such as use and safekeeping of resources and assets so that certain objectives can be reached (strategic, operational, reporting and compliance)
2. Controlling the *quality of the information* that managers use in decision making (e.g. regarding use of resources) or report to external stakeholders (e.g. relating to compliance).

Given the importance of information and information technology in achieving company objectives (ITGI 2004), this dimension needs to be included when defining and researching internal control (Granlund & Mouritsen 2003, Sutton 2005). The risk management perspective inherent in COSO sees information as critical if the organization is to achieve its objectives through decision making at all levels as well as reporting quality information to external stakeholders. The quality of information for external and internal decision-making and the controls to secure this information quality is crucial if the company is to achieve its objectives as defined in the COSO framework. Information quality is not an objective concept but includes the characteristics of the user of the information, the context it is used in as well as the accuracy, integrity, reliability, timeliness and accessibility of the information (Wang & Strong 1996). Other frameworks that have addressed information quality and information systems are SysTrust and WebTrust from the American institute for Certified Public Accountants (AICPA) (AICPA & CICA 2003).

Both the literature review and the interviews show business process risk management and internal controls being linked to information technology generally and to enterprise resource planning (ERP) systems specifically. For example, including ERP systems and accounting information systems in compliance management efforts is crucial, particularly in complying with the Sarbanes-Oxley Act. The PCAOB Auditing Standard states that "the nature and characteristics of a company's use of information technology in its information system affect the company's internal control over financial reporting" (ITGI 2004: p. 12). Issues integrating risk management, compliance and internal controls in this context would include:

1. Integrating risk assessment of control, intentional and unintentional failures in business processes leading to incorrect data entering the system
2. Considering the possibility of automated controls in ERP systems, replacing or supplementing manual controls
3. Considering more preventive controls, replacing or supplementing detective controls.
4. Focusing on documentation of controls as a crucial ingredient in control assessments.
5. Considering the role of internal auditors and external auditors regarding, for example, testing of controls.

Summing up, business process risk management, internal controls and compliance are closely related. Risk management is to a large extent about developing, implementing and operating controls for mitigating, avoiding or transferring risk. All are linked to corporate strategy and corporate objectives (strategic, operational, reporting and compliance). Risk management and internal controls take place in the context of business processes and in an information system environment. This is shown in Figure 1.

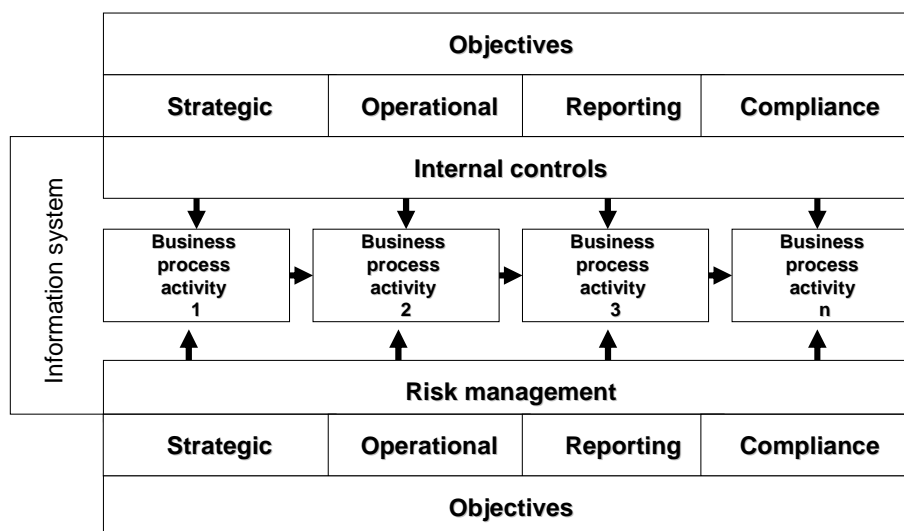


Figure 1: Integrating Risk management, compliance and internal control in the context of business processes

5. Conclusions and a research agenda

From the literature review and the interviews, it is clear that risk management, compliance and internal control are becoming more integrated in a variety of business contexts.

Combining and synthesising the literature review and the interviews, we present an overall list of research questions that seem relevant for further research into the integration between risk management and management control. The questions below are on a general level and would need to be specified in a potential research setting.

Business process risk management

There is a need for research within modelling risk processes in connection with business processes, researching standardisation of business process risk management and exploring the impact of various contingency factors on business process risk management. Some research questions that need to be addressed are:

1. How do companies define and conceptualize business process risk and how do they select controls to address that risk?
2. How is a shared understanding of the principal strategic, financial and regulatory risks facing the organization achieved?
3. How can business process models be integrated with models of control processes?
4. How can risk be modelled so as it can be integrated in business process management models?
5. How is efficiency and effectiveness of a business process risk management system measured?
6. How does the risk portfolio of a company change with the presence of automated controls?
7. How are ERP systems included in business process risk management and what controls are adopted?
8. What risk management practices are in place regarding reputation damage threats and what controls are in place?

Compliance risk management

There is a need for research regarding compliance on a broader level and not just regarding each corporate function. This would entail a focus on the general processes involved in compliance, how these processes reach across organizational and geographical boundaries as well as exploring contextual influences on compliance and compliance performance. Research questions include:

1. What types of compliance processes are there and how can these be modelled?
2. How is the organisational responsibility for global, regional and local compliance evolving?
3. How are global compliance issues managed in companies?
4. Who are the various constituencies that have an interest in compliance performance and how do companies address these?
5. What roles and responsibilities for compliance requirements are there in companies and what practices are evolving?
6. What would a general compliance process reference model look like?

7. How can companies develop early warning systems for compliance?
8. How can the costs of non-compliance be measured?
9. Does a good compliance record pay off in higher share prices?
10. How do companies use IT to support and secure compliance and how can IT support compliance most effectively?
11. Is compliance more cost effective in companies with ERP systems than companies without?

Internal control development

There is a long tradition for research into internal controls in the context of management accounting, financial reporting and general management. However, little research has focused on internal controls specifically in the context of risk management and business processes. Some questions that could be addressed are:

1. How are internal control systems currently evolving and what life cycle maturity stages do these go through?
2. How do companies interpret the COSO control framework in the context of SOX? Is there a common understanding of the requirements or are there differences?
3. How do different control frameworks compare including COSO, COBIT, WebTrust, SysTrust etc.?
4. How do companies assess and develop company wide internal controls?
5. What preventive controls are available to companies and how do these differ regarding contingent variables such as size, technology, industry and structure?
6. How can the efficiency and effectiveness of an internal control system be assessed and compared, for example, between different business units?
7. What is the cost efficiency of implementing the controls defined by COBIT compared to risk assessments and control effectiveness?
8. Do ERP systems mean more efficient and effective internal control practices?

Overall, it can be concluded that intersection between risk management, business process management and compliance is very much in need of more investigation, both academic research (i.e. for the sake of understanding organisational and institutional practice) as well as practical research for contributing to the development of better solutions, guidelines and frameworks for companies.

References

- Adams, S. (2004). Age discrimination legislation and the employment of older workers. *Labour Economics*. Vol. 11 (2004): 219–241
- Ahrens, T. & C. S. Chapman (2004): Accounting for flexibility and efficiency: A field study of management control systems in a restaurant chain, *Contemporary Accounting Research*, volume 21, issue 2: 271-301
- AICPA & CICA (2003). *Trust Services Principles and Criteria: Incorporating SysTrust and WebTrust*. American Institute of Certified Public Accountants, Inc. and Canadian Institute of Chartered Accountants. Available from <http://www.webtrust.net/downloads/WT.TrustServices.pdf>. Accessed 3/5 2006.
- Anthony, R. & V. Govindarajan (2003). *Management Control Systems*. New York: MacGraw Hill.
- Ashford, N. & C. Caldart (2001). Negotiated environmental and occupational health and safety agreements in the United States: Lessons for policy. *Journal of Cleaner Production*. Vol. 9 (2001): 99–120.
- Baker R. W. E. Bealing Jr. D. A. Nelson A. Blair Staley (2006). An Institutional Perspective of the Sarbanes-Oxley Act. *Managerial Auditing Journal* 21(1): 23-33.
- Ballou, B., Godwin, N. H. and Tilbury, V. (2000) Riverfest: Managing Risk and Measuring Performance at Little Rock's Annual Music and Arts Festival. *Issues in Accounting Education*. Vol. 15: 483-512.
- Booker, S.; J. Gardner; L. Steelhammer; J. Zumbakvte (2004). What Is Your Risk Appetite? The Risk-IT Model. *International Information System and Control Journal*. Vol 2: pp. 5-9.
- Borodzicz, E. P. (2005). *Risk, Crisis and Management*. New York: John Wiley & Sons.
- Byington J. R. & J. A. Christensen (2005). SOX 404: How do you control your internal controls? *Journal of Corporate Accounting and Finance*. May/June 2005: 35-40.
- Cannon D. M. & G. A. Growe (2004). 'SOA Compliance: Will IT Sabotage your Efforts?' *Journal of Corporate Accounting & Finance*. July/August 2004: 31-37.
- Charette, R. (1990). *Applications Strategies for Risk Management*. McGraw-Hill, New York.
- Chenhall, R. (2003). Management Control Systems Design Within its Organisational Context: Findings from Contingency-based research and Directions for the Future. *Accounting, Organizations and Society*. Vol. 28 (2-3): 127-168.
- COSO - Committee of Sponsoring Organizations (COSO) (1992). *Internal Control - Integrated Framework*, www.coso.org. accessed February 26 2006
- COSO - Committee of Sponsoring Organizations (COSO) (2004). *Enterprise Risk Management*, www.coso.org. Accessed February 26 2006.
- CRA - Charles River & Associates (2005). *Sarbanes-Oxley Section 404: Costs and Remediation of Deficiencies: Estimates from a Sample of Fortune 1000 Companies*. Available from <http://www.crai.com>. Accessed 1/3 2006
- Davenport, T. H., J. G. Harris & S. Cantrell (2004): Enterprise systems and ongoing process change, *Business Process Management Journal*, Vol. 10 (1): 16-26.

- DrugResearcher (2004) Non-compliance costs drug industry dear.
<http://www.drugresearcher.com/news/ng.asp?id=54525-non-compliance-costs>. Accessed May 5 2006.
- Emmanuel, C., D. Otley & K. Merchant (1995). *Accounting for Management Control*. London: Chapman & Hall.
- Flamholtz, F. & T. K. Das (1985). Toward an Integrative Framework of Organizational Control. *Accounting Organizations and Society*. Vol 10 (1): 35-50.
- Gangadharan, L. (2006). Environmental compliance by firms in the manufacturing sector in Mexico. *Ecological Economics* – In Press 5/5 2006.
- Gemmer, A. (1997). Risk Management: Moving Beyond Process. In *Computer*. Vol. 30: 33 - 43.
- Granlund, M. & J. Mouritsen (2003). Introduction: problematizing the relationship between management control and information technology. *European Accounting Review*. Vol 12 (1): 77-83
- Harmon, P. (2003). *Business Process Change*. Morgan Kaufman Publishers. San Francisco.
- IMJ - Information Management Journal (2004). AMR Research 2004: Compliance Costs Are Rising. *Information Management Journal*. November/December: 6.
- ITGI – IT Governance Institute (2004). *IT Control Objectives for Sarbanes-Oxley*. Rolling Meadows (IL): IT Governance Institute Available from www.isaca.org. Accessed 1/3 2006.
- ITGI – IT Governance Institute (2005). *Control Objectives for Information and related Technology*. Rolling Meadows (IL): IT Governance Institute. Available from www.isaca.org. Accessed 1/3 2006.
- Jaafari, A. (2001). Management of Risks, Uncertainties and Opportunities on Projects: Time for a Fundamental Shift. *International Journal of Project Management*. Vol. 19: 89-101.
- Kendal K. (2004). A 10 Step Sarbanes-Oxley Solution. *Internal Auditor*. December 2004: pp. 51-55.
- Kliem, R. L. (2000) Risk Management for Business Process Reengineering Projects, *Information Systems Management*. Vol. 17: 71-73.
- March, J. G. & Z. Shapira, Z. (1987). Managerial Perspectives on Risk and Risk Taking. *Management Science*, Vol. 33: 1404-1418.
- Markham, R. & P. Hamerman (2005). *The Forrester Wave™: Sarbanes-Oxley Compliance Software. Evaluation Of Top SOX Software Vendors Across 58 Criteria*. Available from www.forrester.com. Accessed May 3 2006
- Matyjewicz G. & J. D'Arcangelo (2004). Beyond Sarbanes Oxley. *Internal Auditor* October 2004: 67-72.
- Merchant, K. A. & Van der Stede, W. A. (2003). *Management Control Systems: Performance Measurement, Evaluation and Incentives*. London: Pearson/Prentice Hall.
- Otley, D. & A. Berry (1980). Control, organization, and accounting. *Accounting, Organizations and Society*. Vol 5 (2): 231-246.
- Rikhardsson, P. C. Rohde, A. Rom (2005). Exploring Enterprise Systems and Management Control in the Information Society: Developing a Conceptual Framework. Presented at the 6th International Research Symposium on Accounting Information Systems, December 10-11, 2005, Las Vegas, USA.
- Shue L. (2004). Sarbanes Oxley and IT outsourcing. *Information System Audit and Control Association*. Vol. 5: 5-9

- Simons, R. (1995). *Levers of Control*. Boston, Mass.: Harvard Business School Press.
- Simons, R. (2000). *Performance measurement and control systems for implementing strategy: Text & cases*, Upper Saddle River: Prentice Hall.
- Stephens, D. (2005). The Sarbanes-Oxley Act: Record Management Implications. *Records Management Journal*. Vol. 15(2): 98-103.
- Suh, B. and Han, I. (2003) The IS Risk Analysis Based on a Business Model. *Information & Management*, 41: 149-158.
- Sutton, S. (2005). The Role of AIS in guiding Practice. *International Journal of Accounting Information Systems*. Editorial. Vol 6. (2005): 1-4.
- Testa, B. (2005). The high cost of noncompliance. *Electronic Business Online* <http://www.reed-electronics.com/eb-mag/article/CA6252379?pubdate=9%2F1%2F2005>. Accessed May 4 2006.
- Waldman, M. (2005). Operationalizing Sarbanes-Oxley: How to Leverage Sarbanes-Oxley to Add Value to Business Operations. Percipio Consulting Group. Available from <http://www.percipiogroup.com>. Accessed May 1 2006.
- Wang, R. & D. Strong (1996). Beyond Accuracy: What Data Quality Means to Data Consumers. *Journal of Management Information Systems*. Vol. 12 (4): 5-34.
- Ward, S. and Chapman, C. (1994) Transforming Project Risk Management into Project Uncertainty Management. *International Journal of Project Management*. Vol. 21: 97-105.
- Yu, F.-J., Hwang, S.-L. and Huang, Y.-H. (1999) Task Analysis for Industrial Work Process from Aspects of Human Reliability and System Safety. *Risk Analysis*. Vol. 19: 401-415.
- zur Muehlen, M. & M. Rosemann (2005). Integrating Risks in Business Process Models. Presented at the *16th Australasian Conference on Information Systems*, 29 Nov – 2 Dec 2005, Sydney.