5-2012

A Literature Review on Operational IT Risks and Regulations of Institutions in the Financial Service Sector

Stefan Bauer
Vienna University of Economics and Business, stefan.bauer@wu.ac.at

A Literature Review on Operational IT Risks and Regulations of Institutions in the Financial Service Sector

Stefan Bauer
Vienna University of Economics and Business
stefan.bauer@wu.ac.at

Abstract
In the last decade public authorities have put many global and local regulations for financial institutions into practice. Several of these regulations concern operational IT risks of financial institutions. For financial institutions using the Advanced Measurement Approach operational risk is important to calculate their minimum capital requirements. The objective of this paper is to provide a comprehensive literature review concerning operational risks, regulations and financial institutions. 37 scientific articles were analyzed and categorized by Basel II operational risk definition. Research gaps were identified in particular regarding the role of IT to balance of minimum capital requirements, the use of operational risk information systems and the discovery of toxic combinations of privileges within and outside of IT systems and services.

Keywords
Operational Risk, IT-Risk, Regulation, Basel II, SOX, Solvency II, banking sector, insurance sector, financial sector, Literature Review

1. Introduction
There has been growing interest in operational risk management. The main reasons for this are that numerous financial institutions reported operational losses and the recent financial crisis (Acharyya 2010, Goldstein et al. 2010). For example, UBS incurred an operational loss due to fraudulent behavior of one of its traders (BBC 2011). Another example displaying the severeness of the turmoil in the financial service industry even better is that, in 2008, 119 banks reported operating losses to the Standards Implementation Group (SIGOR) amounting to a total sum of € 59.6 billion (Basel Committee 2009). As demonstrated by these examples, operational loss events are multifaceted and thus, complex. They range from categories such as internal and external fraud to business interruptions caused by system failure (Goldstein et al. 2011). Given the inherent complexity of these events, operational risk management is a topic of interest for future research.

International public authorities have been implementing a vast amount of regulations to prevent the economy and, especially, the financial sector, from incurring operational losses in the future. In the early 2000s (e.g. Enron, Tyco, WorldCom), the US government passed the Sarbanes Oxley Act (SOX) (United States Congress 2002). The Sarbanes Oxley Act is compulsory for all companies which are listed on a US stock exchange. SOX should have enhanced public confidence in financial reporting, the auditing professions, and financial

markets (Forcht & Luthy 2006). The European Parliament has passed a directive similar to SOX, called EUROSOX, which was incorporated by all EU members (The European Parliament and the Council of the European Union 2006). In addition, Basel II was published by the Basel Committee on Banking Supervision (Basel Committee 2006). Since 2007, Basel II has been compulsory for all credit and financial service institutions in the European Union (Moosa 2007). Basel II sets minimum capital requirements for banks (Jobst 2007b). Currently, Basel III is being implemented with an aim to further strengthen the resilience of the banking sector (Härle et al. 2010).

The minimum capital requirements for operational risks are determined through three different measurement approaches, causing variations in the minimum level of capital required (Mikes 2009). Because of the link between operational risk and minimum capital requirements, banks are interested in the reduction, transfer, or elimination of operational risks (Flores et al. 2006). With the Solvency II directive, European insurance companies are going to face a regulation similar to Basel II, because Solvency II also uses operational risks to determine solvency capital requirements (Acharyya & Johnson 2006). Figure 1 gives a summary of several selected regulations and standards. Through this wave of new regulations in the last decade, operational risk management of financial institutions has become more challenging, but at the same time, more important than ever before.

The purpose of this paper is to present an overview of academic literature on the topic of operational IT risk management in financial institutions. For financial institutions the link between operational risk management and minimum capital requirements has received considerable attention (Jobst 2007b). The focus of this paper is the academic literature starting in 2002, because the most important regulations (e.g. SOX, Basel II) were put into practice from this period onwards. A systematic literature review is useful to offer a clear view on operational risk management and regulation. In this paper, I will focus on the information technology aspect of operational risk management, because there is a lack of detailed research on IT operational risk (Goldstein et al. 2011). Because information is the most important asset of financial institutions, information technology becomes necessary for survival (Goldstein et al. 2011).

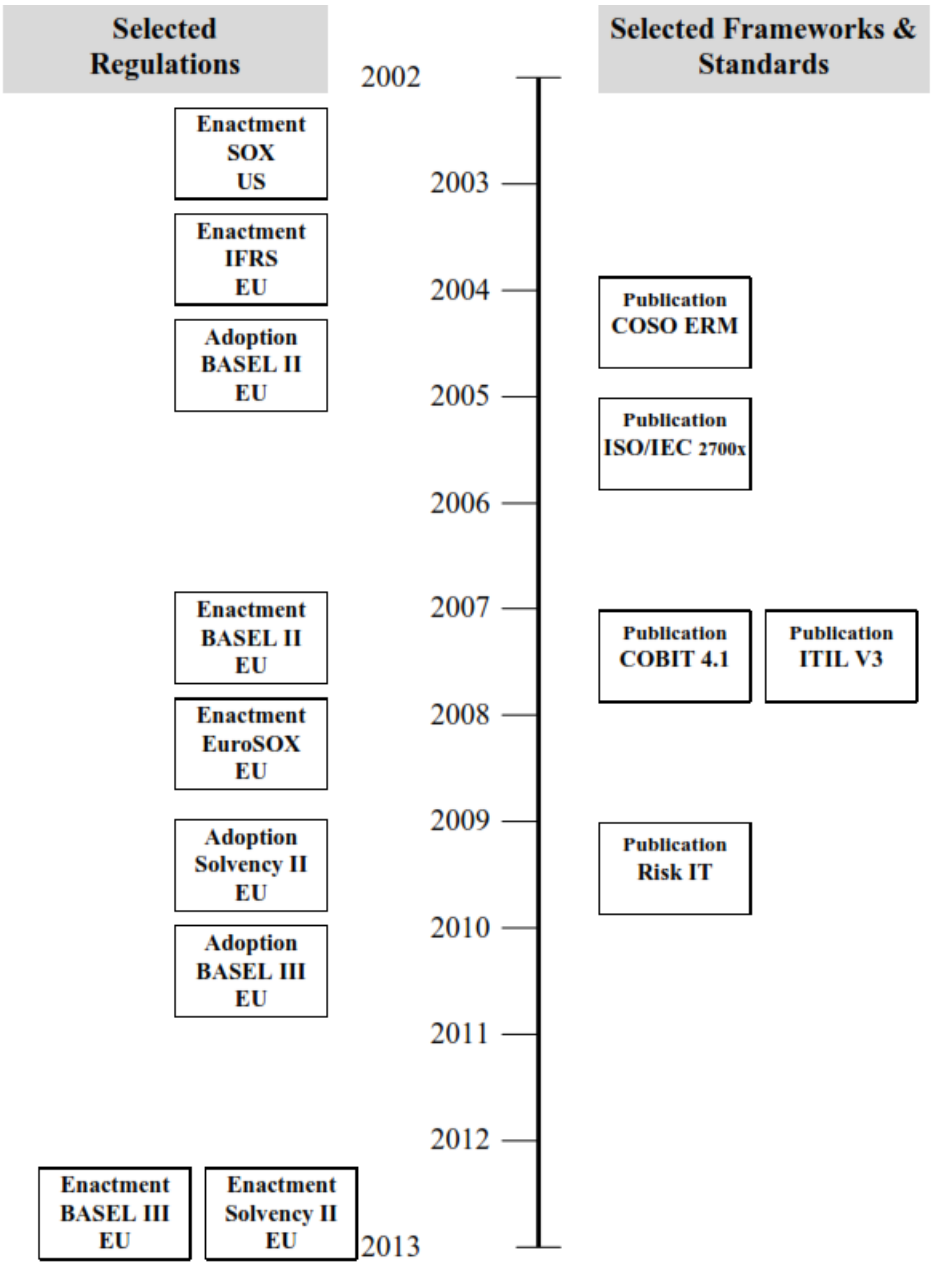

Figure 1: Selected regulations, standards and frameworks and their enactment periods

The paper is divided into five sections. The paper begins by briefly describing the significance of the topic for scientific research and describes methodological aspects. The second section considers definitions and boundaries of current research. In the third section, the methodological framework is discussed. The research process is visualized through Figure 2. In section four, the main concepts are analyzed. The concluding section summaries literature gaps.

2. Theoretical background

Several authors have stated that the academic literature on operational risk in the financial sector is often inconsistent and takes several different views (Acharyya 2010, Moosa 2007). Some authors of the late 90's saw operational risk as the residual that is not faced by credit or market risk (Wahlström 2006). According to Moosa (2007) this approach was too broad and not specific enough. Most of the researched articles for this literature review refer to the Basel II operational risk definition.

In this paper, the term operational risk is defined as "the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events. This definition includes legal risk, but excludes strategic and reputational risk" (Basel II 2004, p.137). At this point it is important to consider that operational risks have three dimensions. There is the cause, the event, and the consequence (Mossa 2007). The Basel Committee of Banking Supervision classifies operational risk on the event dimension, thus this research also discuss the event taxonomy. The operational risk definition from Basel II excludes strategic risks. Acharyya (2010) mentioned that this exclusion doesn't reflect reality. The author studied the relationship between strategic risk in the enterprise risk management framework and operational risk in financial institutions. He found that strategic management influences many areas where operational risks occur (Acharyya 2010). Because of this reason, this paper extends the Basel II taxonomy with strategic risk.

So far little attention has been given to information technology aspects of operational risks, which occur in every event type category of Basel II operational risk definition (cf. Goldstein et al. 2011). The term 'IT operational risk' is generally understood as "any threat that may lead to the improper modification, destruction, theft, or lack of availability of IT assets" (Straub & Welke 1998, p.442). In this research the term is also used according to Goldstein et al. (2011), who distinguishes between data-related IT operational risk and function-related IT operational risks as follows: "Data-related IT operational risk is any threat to the confidentiality of data assets that can result in the disclosure, misuse, or destruction of these assets. Function-related IT operational risk is any threat to the availability or to the integrity of functional IT assets" (Goldstein et al. 2011, p.610). Thus, this literature review also focuses on the differences between approaches on operational risks in the direction of IS/IT.

The investigated regulations are comprehensive and therefore, this review concentrates on specific sections of the analyzed regulations. Basel II consists of three pillars. The present paper gives attention to the first pillar, and within the first pillar on operational risks, and not on credit or market risks (Flores et al. 2006). Section 404 is for the purpose of this paper the most interesting section of SOX, because this section discusses the effectiveness of internal controls. Internal controls and in series operational risk information systems are of increasing importance in consideration of the Advanced Measurement Approach of Basel II (Koutoupis & Tsamis 2008). The relevant part of Solvency II focuses on new methods for calculating capital requirements and new internal control systems (Bónson et al. 2010). After the definitions and boundaries of the topic, the next step is to explain the research methodology.

3. Methodology

The present paper provides a literature review according to the methodology of Watson and Webster (2002). As can be seen from Figure 2, this study consists of three fundamental parts: research definition, research methodology, and research analysis. The paper starts with the research definition, which is presented in the introduction and in the second section. In the first sections the research area is identified, the research goals are formulated, and the scope is defined. Thereafter, follows the research methodology in section 3. The analyzed papers were selected through a keyword based research in the following academic meta-databases: Web of knowledge (SSCI), ProQuest, IEEE computer society, Science Direct, Springer Journals, Emerald online, ACM Digital Library, and Google scholar. In addition, the journal database of the Journal of the AIS was searched. The used keywords and how they were applied are seen in Figure 2. Not a simple Boolean AND operation was applied. Articles were manually screened for relevance.

The research framework (Figure 2) shows a list of the used keywords. Furthermore, during the research process, the identified papers were used to find new relevant literature following a snowball system. This causes the discovered literature to be quite divers. The criteria for the acceptation of an article were that the articles had to be related to all of the three research interests: banking/insurance sector, regulation (Basel II, SOX, Solvency II) and IT operational risks. The researched papers must have been published between 2002 and 2011. This ten year period seems to be appropriate, because as seen in Figure 1, within this period the most relevant new regulations such as SOX or Basel II were put into practice.

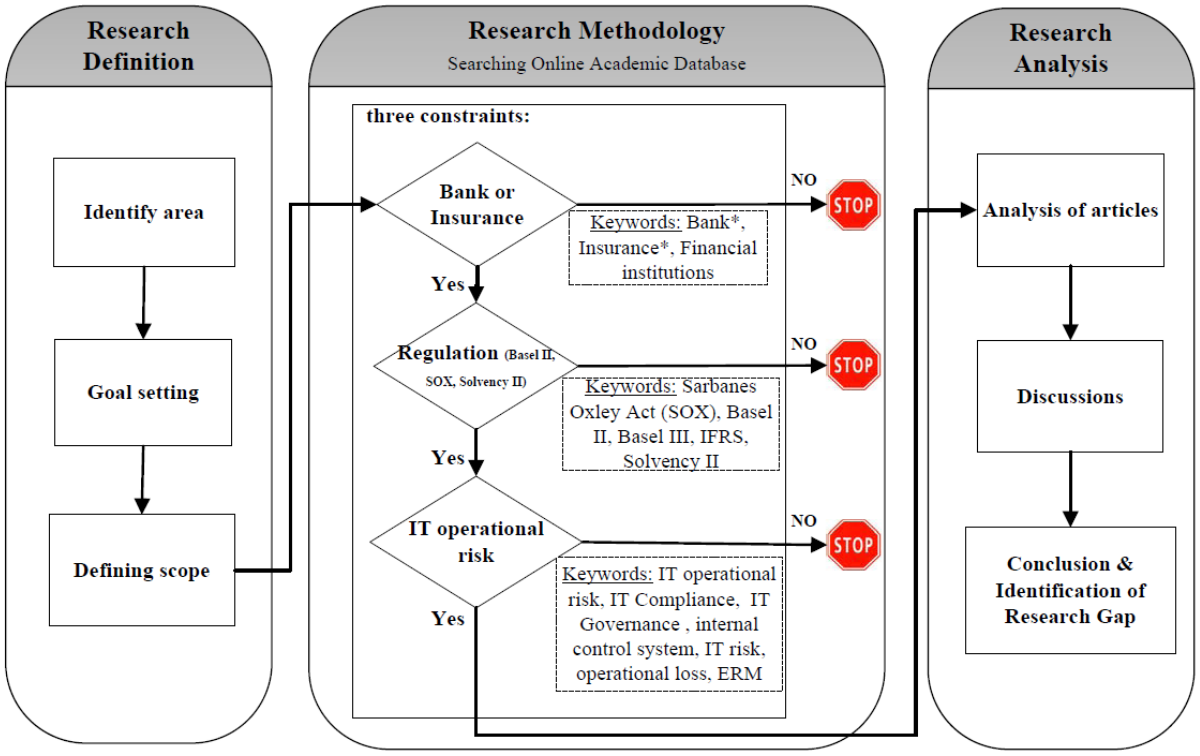

Figure 2: Methodological Framework

4. Analysis of the Literature

This chapter presents the analysis of the literature. The first subsection investigates the quality of journals publishing identified articles. In Section 4.2. the frequency of occurrence of regulations and sectors is shown. In the next subchapter the articles are evaluated statistically by frameworks and standards. The methodologies of the researched articles are described in Section 4.4. The main concepts of the articles are characterized in Section 4.5. The subchapters of Section 4.5. investigate the main findings and interesting research areas of the articles. The section is divided into five subchapters and begins by analyzing the articles classified as the holistic view of operational risk, followed by the measurement and reporting approach. The paper goes on with a critical review of articles relating to organizational complexity and risk from people, systems and processes, and strategic risks. Section 4.6. discusses the Basel II Loss Event Type Classification. Finally, the last subchapter looks at the differences between banking and insurance sectors.

4.1. Quality of Journals

Altogether this research focuses on 37 scientific articles of different quality. A method to identify the quality of the articles is to categorize them by journal quality. Quality is determined by the 'Academic Journal Quality Guide' (Harvey et al. 2010). The journal quality ranking reaches from one to four stars. One of the researched 37 articles was published in a four stars top journal, and further six articles were issued in three stars journals. Five papers were found in one star journals and eight articles were published in journals that were not classified by the ranking. 17 articles are published in conference proceedings of information management related conferences. These results may be interpreted that there is a lack of publications on the research topic in excellent and very good journals.

4.2. Classification of Articles by Regulation and Sector

This section deals with the classification of articles by regulation and sector. Figure 3 illustrates the frequency distribution of these articles according to different regulations and sectors.

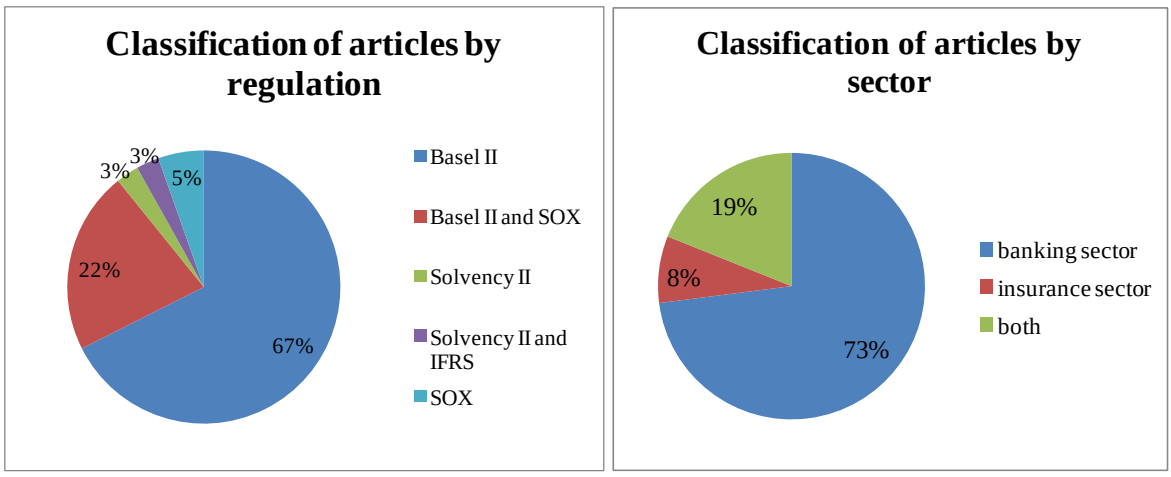

Figure 3 Occurrence of Articles in Sectors, differentiated by Regulations

As can be seen from Figure 3, Basel II appears in 89% of the researched articles. 67% of the articles refer only to Basel II and 22% discuss SOX and Basel II. Exclusive SOX discussions were found in 5% of the articles. There is a lack of literature on Solvency II, as just 6% of articles deal with this regulation. The reason for this result may be that Solvency II is relatively new, because Solvency II was adopted in 2009 and it is going to be enacted in 2013.

Another gap of literature regards Basel III, which was not found in academic literature, but in articles of consulting companies. (Härle et al. 2010)

From the data in Figure 3, it can be concluded that most literature deals with the banking sector or the banking and the insurance sector. 73% of the articles refer to the banking sector and 19% to both, the banking and the insurance sector. Only 8% of the articles discuss the insurance sector exclusively. This frequency distribution may also be explained by Solvency II's relatively recent implementation.

4.3. Classification of Articles by Frameworks and Standards

There is a substantial amount of research that has discussed standards for risk management (e.g. COSO, Risk IT, ISO 27000, CAS) or government frameworks (e.g. CobiT). Eight articles refer to the COSO risk management framework and five articles mention the CobiT framework. Four articles discuss different ISO standards. Risk IT and ITIL were stated both each three times. Some standards were used only one or two times (e.g. CAS, process reference model). As several articles demonstrate, standards and frameworks are very useful to manage operational risks successfully. (Forcht & Luthy 2006, Pardo et al. 2011)

4.4. Applied Research Methodologies

Methodologies are indicators to analyze the deepness of research of the underlying topic. Twenty-two of the researched articles are classified as an exploratory or descriptive study. These articles explore or describe their research aims. Furthermore, there are ten case studies and two field studies, which investigated their research topic by one or more cases. Only two of the thirty-seven researched articles are event studies, which rely on real operational risk or operational loss data from OpVar and FIRST databases (Cummins et al. 2006, Goldstein et al. 2011). One article is a multi-method study, containing qualitative and quantitative research. In interpreting these findings, we have to consider that in the financial sector quantitative studies are hard to execute, because operational risks and operational losses are sensitive topics for banks and insurance companies. Previous research has neglected to provide comprehensive quantitative research on this topic.

4.5. Basel II Classification

Table 1 provides an overview about the grouping of the investigated literature. The research articles were classified by approaches abstracted from Basel II definition of operational risk, extended by strategic risks. Operational risks can be divided in internal and external loss events. In this review there is no paper which explicitly refers to external loss events, thus there is no section for this loss type.

Article	Holistic	Process	People	Systems	Measure	Strategic
Abdullah et al. (2011)					X	
Acharyya (2010)						X
Acharyya and Johnson (2006)	X					
Atkinson et al. (2006)				X		
Ayerbe et al. (2010)			X			
Bernard et al. (2007)		X				
Bonson et al. (2010)					X	
Cummins et al. (2006)	X					
Dalla Valle and Giudici (2008)					X	
Flores et al. (2006)					X	
Forcht and Luthy (2006)					X	
Gao and Sun (2010)			X			
Gewald and Hinz (2004)		X				
Goldstein et al. (2008)	X					
Goldstein et al. (2011)				X		
Hinz (2005)				X		
Jobst (2007a)					X	
Jobst (2007b)	X					
Koutoupis and Tsamis (2008)					X	
Locher (2005)					X	
Locher et al. (2004)					X	
Longo (2009)	X					
Mikes (2009)						X
Moosa (2007)	X					
Neirotti and Paolucci (2007)				X		
Oh et al. (2007)	X					
Pardo et al. (2011)	X					
Romanovs et al. (2008)				X		
Rotaru et al. (2009)					X	
Sinclair et al. (2008)			X			
Spears and Barki (2010)			X			
Supatgiat et al. (2006)		X				
Svata and Fleischmann (2011)	X					
Wahlström (2004)		X				
Weiß and Winkelmann (2011)		X				
Yang et al. (2010)	X					
Zoet et al. (2009)		X				

Table 1 Articles classified by concepts of Basel II

The next subsections discuss the articles of Table 1 according to the introduced Basel II classifications.

4.5.1. Holistic View

Several recent studies have focused on operational risk management in a holistic view (Mossa 2007, Svata & Fleischmann 2010). These articles discuss economic effects or new knowledge about operational risks in general. More sophisticated methods would be required to fully understand the gap between real operational losses and estimated operational risks. This uncertainty leads to a dilemma; choosing between too little or too much capital requirements. A shortage of capital could cause a collapse of the bank and excessive capital could reduce competitiveness and financial leverage (Flores et al. 2006). As Oh et al. (2007) has noted, efficient risk management in financial institutions can arise from reduction in compliance costs or from preventing loss from fraud (Oh et al. 2007).

4.5.2. Operational Risk Measurement Approaches and Operational Risk IS

Basel II (2004) defines in opposite to the old 1988 Basel Capital Accord three measurement approaches for operational risk capital requirements (Jobst 2007a). There is the Basic Indicator Approach, the Standard Approach, and the Advanced Measurement Approach. The Basic Indicator approach and the standard approach are static and easy to measure, because they use fixed percentages of banks' gross income to compute capital charges for operational risk (Abdullah et al. 2011, Flores et al. 2006, Jobst 2007b). Thus, an over- or underestimation of operational risk is likely (Flores et al. 2006). Both approaches are useful for small banks (Dalla Valle & Guidici 2008). Several authors have suggested that the Advanced Measurement Approach could lead to an efficient risk management and reduce capital requirements (Locher 2005, Forcht & Luthy 2006). The Advanced Measurement Approach could be implemented in three different ways: the scenario-based approach, the scorecard approach and the loss distribution approach (Locher et al. 2004). These approaches rely on empirical estimates of operational losses.

The estimation of operational losses is very difficult for financial institutions, because there is a lack of operational loss data (Dalla Valle & Guidici 2008). Because of this, the Advanced Measurement Approach asks for an operational risk information system to identify risks and capital requirements (Flores et al. 2006). Information technology is the key enabler of operational risk management strategies (Oh et al. 2007). The study of Flores et al. (2006) focuses on the benefits of an effective operational risk information system. Such an information system could mitigate risks, thus reduce equity requirements and therefore, the financial institution could be more competitive. There is a trend to the standardization of reporting (Bónson et al. 2010). The Committee of European Banking Supervisors (CEBS) forces a XBRL-based project called COREP-FINREP, which tries to implement banking risks and international accounting regulation (Bónson et al. 2010). As Acharyya & Johnson (2006) has noted, the solution in reporting operational risks is to encourage the employees or business entities to give notice of a loss event so that a database and an information system could be established.

4.5.3. People and organizational complexity

Management culture, organizational structure and the personal opinions of employee's influences operational risks management (Méndez et al. 2010). Sinclair et al. (2008) discovered the organizational complexity and points out toxic combinations of privileges. "A toxic combination is a conflict of system access permissions that allows a user to break the law, violate rules of ethics, damage customers' trust, or even create the appearance of impropriety." (Sinclair et al 2008, p. 167) This problem occurs in the case of promotions, if an employee has access to write checks and afterwards he would be promoted to a position, where he can delete check writing records (Sinclair et al. 2008). Another problem is the risk

of over-access, which could be mitigated by giving only the right people access to the information they need for their organizational role. Over-access can cause internal fraud and misuse of data (Sinclair et al. 2008). A source of risk could also be that corporate information is consumed out of the companies, because of the easy access to public networks to remote email, smart phones, laptops and tablets (Sinclair et al. 2008).

4.5.4. Systems and Processes

According to Weiß & Winkelmann (2011), there was no business process modeling language which fulfills the requirements of financial institutions. The authors invented a semantic business process modeling language for banks, which considers different views, like the business objective view, the organizational view, and the resource view. For future research, it is recommended to use the business process modeling language of Weiß & Winkelmann (2011).

4.5.5. Strategic

Acharyya (2010) and Mikes (2009) mentioned that strategy and strategic decisions influence the occurrence of operational risks. Mikes (2009) points out that risk identifiers had no influence on strategy or strategic decisions of the organization. This research direction was discussed in many articles relating to aligning IT and strategy, but for the financial industry there is a lack of literature on this research line.

4.6. Basel II Loss Event Type Classification

Several authors investigated the classification of loss event types of Basel II, but only two authors had investigated this classification in detail (Goldstein et al. 2011, Cummins et al. 2006). Goldstein et al. (2011) analyzed data of the FIRST database and pointed out, that 85% of all loss events are allotted to the categories 'external fraud', 'business disruption and system failure' and 'execution, delivery and process management'. Because of the domination of these three event types, future research should concentrate on them. Further Goldstein et al. (2011) mentioned that future research should focus on function-related IT operational risk events, because functional-related events exert on average a greater negative wealth effect.

4.7. Differences between bank and insurance sector

Few authors discuss the differences between banks and insurance companies with different outcomes. For Acharyya (2010) operational risks have had bigger impact on the banking industry than on the insurance industry, because banks face an anytime dynamic payment system in contrast to insurance companies. Otherwise Cummins et al. (2006) found out that if an operational loss occurs, then insurance companies are more affected by a market value reduction than banks. The differences between banking and the insurance sector are discussed poorly in the literature, therefore future research is needed.

5. Conclusion

This research paper identifies areas and issues for further investigation regarding IT risks and regulations of financial institutions. Through a systematic multi-step literature search (Watson & Webster 2002) 37 different articles were identified as being within the scope of this study. These articles were descriptively analyzed according to their focal industry sector (banks or insurance companies), targeted regulation, and control frameworks. In addition, this paper has attempted to classify and discuss the papers according to Basel II guidelines and event loss types. To summarize, the following areas among others seem to warrant more attention related to banks and insurance companies in future work:

- The role of IT to achieve a rational balance of capital requirements (over- or underestimation)
- Design and operationalisation of an effective operational risk information system (Flores et al. 2006)
- Incentives for employees or business entities to disclose weaknesses and loss events (Acharyya & Johnson 2006)?
- More ways to mitigate the rife loss event types 'external fraud', 'business disruption and system failure' and 'execution, delivery and process management' (Goldstein et al. 2011)
- Identification and mitigation of toxic combinations of privileges outside and within IT systems and services (Sinclair et al. 2008)
- Access to corporate information over public networks (Sinclair et al. 2008)

A more systematic analysis of the financial sector of a country or region would be useful to get a realistic picture of specific requirements. According to the identified research methodologies, future research should pay more attention to reliability, e.g., by using more triangulation techniques in case studies, and more comprehensive quantitative research. This seems to be necessary to better understand the substantial risks and their treatment in regard to regulations in the financial sector.

References

Abdullah, M., Shahimi, S., Ghafar Ismail, A. (2011) “Operational risk in Islamic banks: examination of issues”, *Qualitative Research in Financial Markets*, Vol. 3, No. 2, 2011 pp. 131-151

Acharyya, M. (2010) “The role of operational risk and strategic risk in the enterprise risk management framework of financial services firms”, *Int. J. Services Sciences*, Vol. 3, No. 1, pp.79–102.

Acharyya, M. and Johnson, J. (2006) “Investigating the development of enterprise risk management in the insurance industry: an empirical study on four major European insurers.” *The Geneva Papers on Risk and Insurance: Issues and Practice*, 55-80.

Atkinson, C., Cuske, C., Dickopp, T. (2006) “Concepts for an Ontology-centric Technology Risk Management Architecture in the Banking Industry“, *10th IEEE International Enterprise Distributed Object Computing Conference Workshop (EDOCW'06)*

Basel Committee on Banking Supervision (2006) "International Convergence of Capital Measurement and Capital Standards: A Revised Framework, Comprehensive Version." Switzerland: Bank for International Settlements

Basel Committee on Banking Supervision (2009) "Results from the 2008 Loss Data Collection Exercise for Operational Risk" Bank for International Settlements

BBC Business News (2011) “UBS trader Kweku Adoboli charged with fraud”, Retrieved 15 November 2011, from http://www.bbc.co.uk/news/business-14950873

Bónson-Ponte, E., Escobar-Rodíguez, T., Flores, F. (2006) “Operational risk information system: a challenge for the banking sector”, *Journal of Financial Regulation and Compliance* Vol. 14 No. 4, pp. 383-401

COSO (2004) "Enterprise Risk Management Framework", Retrieved 15 November 2011, from http://www.coso.org

Dalla Valle, L., Guidici, P. (2008) “A Bayesian approach to estimate the marginal loss distributions in operational risk management”, *Computational statistics & Data Analysis 52*, pp. 3107-3127

Di Renzo, B., Hillairet, M., Picard, M., Rifaut, A., Bernard, C., Hagen, D., Maar, P., Reinard, D. (2007) “Operational Risk Management in Financial Institutions: Process Assessment in Concordance with Basel II“, *Software Process Improvement and Practice* 12, pp.321-330

Forcht, K., Luthy, D. (2006) “Laws and regulations affecting information management and frameworks for assessing compliance“, *Information Management & Computer Security* Vol. 14 No. 2.; 2006, pp. 155-166

Gewald, H., and Hinz, D. (2004) "A Framework for Classifying the Operational Risks of Outsourcing - Integrating Risks from Systems, Processes, People and External Events within the Banking Industry", *PACIS 2004 Proceedings. Paper 84.* http://aisel.aisnet.org/pacis2004/84

Goldstein, J.; Chernobai, A.; Benaroch, M. (2011) “An Event Study Analysis of the Economic Impact of IT Operational Risk and its Subcategories”; *Journal of the Association for Information Systems*

Goldstein, J. Benaroch, M., Chernobal, A. (2008) “IS-Related Operational Risk: An Exploratory Analysis”, *AMCIS 2008 Proceedings, Paper 89.* http://aisel.aisnet.org/amcis2008/89

Harvey, C., Kelly, A., Morris, H., Rowlinson, M. (2010) “Academic Journal Quality Guide”, *The Association of Business Schools, Version 4*

Härle, P., Lüders, E., Pepanides, T., Pfetsch, S., Poppensieker, T., Stegemann, U. (2010) "Basel II and European banking: Its impact, how banks might respond, and the challenges of implementation", Mc Kinsey&Company

Hinz, D. (2005) “High Severity Information Technology Risks in Finance”, *Proceedings of the 38th Hawaii International Conference on System*

ISO/IEC 27005:2008, Information Security - Security Techniques - Information security risk management.

ISO/IEC, ISO/DIS 31000, Risk Management - Principles and Guidelines on Implementation, Switzerland

IT Governance Institute (2007) “COBIT 4.1.” Rolling Meadows: ISACA, 2007

IT Governance Institute (2009) “Risk IT: Framework for Management of IT Related Business Risks.” *IT Governance Institute* 2009

Jobst, A., (2007a) “It’s all in the data – consistent operational risk measurement and regulation”, *Journal of Financial Regulation and compliance* Vol. 15 No. 4, 2007, pp. 423-449

Jobst, A., (2007b) “The treatment of operational risk under the New Basel framework: Critical issues”, *Journal of Banking Regulation*, Vol. 8, 4 pp.316-352

Koutoupis, A., Tsamis, A. (2009) "Risk based internal auditing within Greek banks: a case study approach", *Journal of Management and Governance* 13: pp.101-130

Locher, C., Mehlau, J., Wild, O., (2004) “Towards Risk Adjusted controlling of Strategic IS Projects in Banks in the Light of Basel II”, *Proceedings of the 37th Hawaii International Conference on System Sciences – 2004*

Locher, C. (2005) “Methodologies for Evaluating Information Security Investments – What Basel II can Change in the Financial Industry”, *ECIS 2005 Proceedings*. Paper 122 http://aisel.aisnet.org/ecis2005/122

Longo, E. (2009) “The Knowledge Management Role in Mitigating Operational Risk”, *European Conference on Intellectual Capital 2009*

Méndez, C., Camargo; G. and Herrera, A. (2010). "Good Practice Guide for Managing IT Risk in Colombian Banking: Specification by Disciplines", *AMCIS 2010 Proceedings*. Paper 511. http://aisel.aisnet.org/amcis2010/511

Mikes, A. (2009) "Risk management and calculative cultures", *Management Accounting Research 20*, pp. 18-40

Moosa, I. (2007) “Operational Risk: A Survey”, *Financial Markets, Institutions & Instruments*, Vol. 16, No. 4, pp. 167-200

Neirotti, P., Paolucci, E. (2007) “Assessing the strategic value of Information Technology:An analysis on the insurance sector“, *Information & Management* 44 (2007) pp. 568-582

Oh, L.; Phua, T.; and Teo, H. (2007) "A Conceptual Model for IT-Enabled Enterprise Risk Management in Financial Organisations", *ECIS 2007 Proceedings. Paper 191.* http://aisel.aisnet.org/ecis2007/191

Pardo, C., Pino, F., García, F., Piattini, M., Baldassarre, M., Lemus, S. (2011) “Homogenization, Comparison and Integration: A Haromonizing Strategy for the Unification of Multi-models in the Banking Sector“, *PROFES 2011, LNCS 6759*, pp. 59-72

Rotaru, K.; Wilkin, C.; Ceglowski, A.; and Churilov, L. (2009) "Towards operational risk-aware information systems: A critical realist perspective", *ECIS 2009 Proceedings.* Paper 106. http://aisel.aisnet.org/ecis2009/106

Sinclair, S., Smith, S., Trudeau, S., Johnson, E., Portera, A. (2008) "Information Risk in Financial Institutions: Field Study and Research Roadmap", *FinanceCom 2007, Montreal, Canada Lecture Notes in Business Information Processing 4* Springer 2008

Straub, D., Welke, R. (1998) "Coping with Systems Risk: Security Planning Models for Management Decision-Making”, *MIS Quarterly* (22: 4, December), pp. 441-469

Svatá, V., Fleischmann, M. (2011) “IS/IT Risk Management in banking industry“, *Acta oeconomica pragensia* 19, 3/2011, ISSN 0572-3043

Supatgiat, C., Kenyon, C., Heusler, L. (2006) "Cause-to-effect operational-risk quantification and management", *Risk Management* 8, pp. 16-42

The European Parliament and the Council of the European Union (2006) "Directive 2006/43/EC of the European Parliament and of the Council," Retrieved 15 November 2011, from http://eur-lex.europa.eu

United States Congress (2002) "The Sarbanes-Oxley Act of 2002", Retrieved 15 November 2011, from http://www.law.uc.edu/CCL/SOact/soact.pdf

Watson, R., Webster, J. (2002) "Analyzing the past to prepare for the Future: Writing a Literature Review", *MIS Quarterly* Vol. 26 No. 2, pp. xiii-xxiii/June 2002

Weiß, B. and Winkelmann, A. (2011) „Developing a Process-Oriented Notation for Modeling Operational Risks – A Conceptual Metamodel Approach to Operational Risk Management in Knowledge Intensive Business Processes within the Financial Industry“, Proceedings of the 44th Hawaii International Conference on System Sciences

Yang, F., LE, Q., Shao, P., Li, D. (2010) “Commentary on the Supervision of Foreign Banking IT Risks”, *International Conference on E-Business and E-Government*