Applications for IT-Risk Management – Requirements and Practical Evaluation

Heinz Lothar Grob, Gereon Strauch, Christian Buddendick
European Research Center for Information Systems,
University of Muenster, Germany
{grob; gereon.strauch; christian.buddendick}ercis.de

Abstract

Nowadays the importance of a dedicated information security management (ISM) is undisputedly. One essential task in realizing a company's ISM is to implement a compulsory operational risk management (ORM) aiming also at ensuring the compliance with certain standards. The risks addressed by ORM prevalently result from information systems. A promising approach is to focus on business processes to combine the technical system focused perspective of security management with the more centralized perspective of operational risk management. Within this paper first we will deliver an introduction an integrated IT risk management and its corresponding decisions. Afterwards we will derive requirements for application systems in order to supporting decisions in IT-Risk Management. For this purpose a catalogue of requirements will be developed. Based on this catalogue software systems for IT security management and operational risk management were examined with regard to their adequacy for decision support in IT-Risk Management.

1. Introduction

By risk – either etymological being descended from the Arabic "rizq" (destiny) or the Latin "risicar" (to transhipa cliff) - the danger of occurring a threat or damage is generally understood. In a broader sense chances as positive deviations from the target value are also subsumed under the risk term, e.g. fiscal risks. Risks can occur within different ranges of the enterprise: Risks within the core business range, risks of fiscal nature (e.g. market-, credit- and asset-risks) and risks resulting from operating activities (operational risks). The necessity for a risk management results exempted from economic considerations just as from different standards and requirements, e.g. such as the Sarbanes Oxley Act [3-6]. Especially financial service providers are obligated to establish a differentiated risk management considering operational risks above all [3, 6]. Even if such far-reaching regulations yet do not apply to other branches of industries, it is expected to be so in the future in future [7].

In the following we will focus on the management of operational risks, which are defined as the "danger of immediate or mediate losses, which occur due to the inadequacy or failure of internal proceedings, humans and systems or external events." [8] On the opposite side there are "chances", so that risk always means the expectation of a potential loss. However, security designates a condition of no danger and no risk and consequently represents the other "side of the medal" [9]. Because of the rising importance of information technology the weight of IT induced risk increases, the importance of operational risks in this context will rise [7, 10]. Admittedly its need of deployment is to be stated regarding the arrangement of an IT risk management in theory and practice. So far, both responsible persons of the operational risk management (ORM) and the information security management (ISM), which normally evolved separately from the content-related and organizational point of view, dealt with the management of IT compelled risks [3]. This was favored by the fact that the appropriate regulations do not state anything about the peculiarity of an IT security or risk management, but only over its necessity [3, 6].

In the following section we will examine the integration potentials of IT security management within the classical management of operational risks need. Afterwards the potentials of application systems

0-7695-3102-4/08 $25.00 © 2008 IEEE
DOI 10.1109/ARES.2008.168

for supporting IT risk management will be outlined. For this purpose a criteria catalogue will be developed to examine the applicability of application systems for the IT risk management. Finally against this background an exemplary analysis of selected software solutions will be conducted. We then conclude with a brief summary and an outlook on further research opportunities.

2. Application Systems to support IT risk management

2.1. Operational risk management and IT - security management

Originally the operational risk management was focused on insuring individual risks. However, risk management systems emerged, which focus on the disposition of aggregate risks and therefore have a strong reference to business processes and a top-down alignment [3]. On that level governance and guidance by the allocation of bare resources are achieved in order to minimize the risk from the company's point of view. This perspective is insufficient when it comes to the management of individual risks on a low aggregation. In particular the management of IT risks cannot be achieved on this level, because the contribution of IT to business processes can hardly be identified from a top-down view [3]. Furthermore the identification and analysis of these risks require the expertise of specialists, which usually are not centrally available [11, 12].

In contrast, a specialized information security management (ISM) emerged which focuses on a faultless service of the companies information system. The ISM traditionally focuses on the consideration of technical systems. Technical systems can cause operational risks for business processes, therefore it is essential to identify these IT related risks and define adequate countermeasures [2]. This bottom-up-approach results in an organizational structure, which finally ends in a bounded point of view [3, 11]. For this purpose this function is usually allocated nearby the system activity level, in order to guarantee that the necessary high competence in the treatment of the specific IT risks is available [11]. Besides conceptual fuzziness existing, the analysis of threats within the scope of ISM occasionally is called risk management [13]

From the isolated point of view of both perspectives on the one hand side ISM and on the other hand side ORM it can hardly be identified, how IT risks affect the aggregate risk disposition of a company [14]. While the ISM, as shown in figure 1, focuses on the systems and therefore can better capture possible threats, from the ORM's point of view the overall amount of damage resulting from the impacts on the business processes can be identified [2]. The management of operational risks (ORM) and the information security management (ISM) therefore need to be aligned functionally, which has not ascertained in theory and practice yet [3, 14]. Due to the integration of a dedicated IT-risk management the governance of the disposition of entrepreneurial risk with regard to economical criteria is possible [13]. At the same time neither the ISM shall be associated with ORM nor shall the linkage over informal ways be made, in order to avoid the disadvantage of a one-sided concentration.

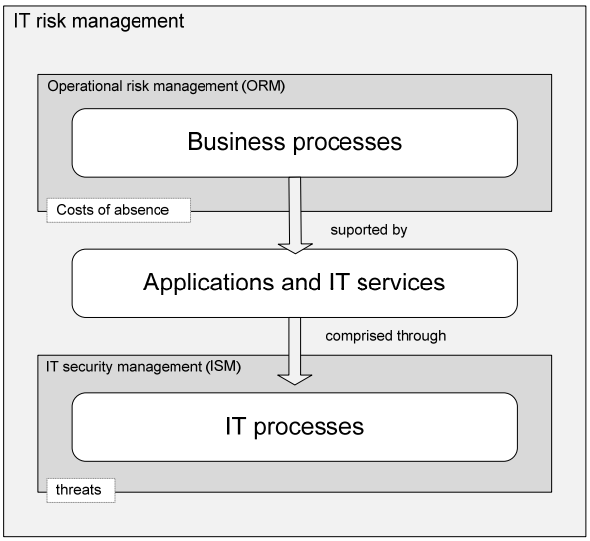

Figure 1. Different focussing of ISM, ORM and IT risk management [2].

In the following the arrangement of information IT support for an integrated IT risk management will be illustrated, which combines the business-process-oriented and the company-wide view. Thereby operational risk management is combined with specific methods and competences of IT security management [10, 14]. By this a contribution to IT security is delivered, which is an expert task, that can be achieved admittedly by the collaboration of all organizational units concerned [11, 15].

2.2. Purpose of IT-risk management

The IT risk management deals with risks resulting from the usage of information systems in a company. The procedure of tasks is oriented at the general process of risk management [1]. On the basis of this process, as shown in figure 2, the advantages resulting from an integration of ORM and ISM are to be demonstrated.

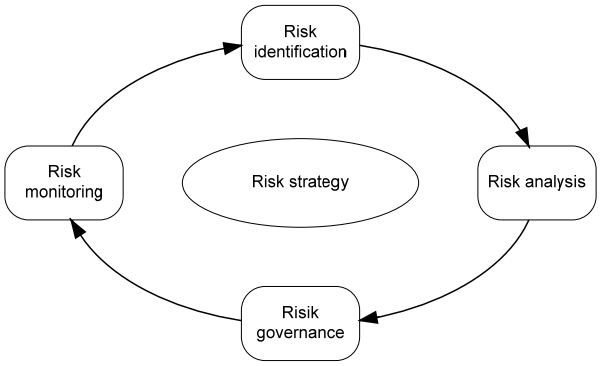

Figure 2. The process of IT risk management [1].

Firstly the goals of IT risk management are to be determined in the context of the risk strategy [1]. According to these goals potential risks for the enterprise need to be identified and to be evaluated by an IT risk analysis [16]. The IT risk analysis serves as a basis for identifying and implementing measures for the risk governance. At this point it is obvious, that this can only achieved with the competence of IT security management. In the classical operational risk management IT risks usually are identified in various categories, but often not quantified [14]. However, the quantification is only possible by the cooperation of central actors and decentralized security experts, since the effects of IT security risks on the business processes need to be assessed in this way [2]. Focusing on business processes has been claimed repeatedly for the IT security management [16-20], but has not been realized in practice yet. A risk governance basically can be achieved by avoiding (refraining from activities), passing (transfer, e.g. insurance), decreasing (protective and preventive measures) or accepting (sustaining) risks [15]. In the context of information systems these measures can be conducted by IT security experts because of their competences [11]. Even so, an overall view has to be taken to allocate resources on the ideal security level from the organization's point of view [3].

The risk control serves as the control of result of the risk governance and is the foundation for planning future measures in terms of a risk controlling. Reports have to be created comprehensively in accordance with the reporting duties. In a largely decentralized IT security management a standardized ascertainment is certainly rare [3]. Furthermore proactive budgeting processes should be designed which account for the defense of potential threats and ensure that no means are assigned after developed incidents.

2.3. Decision support of IT-risk management by application systems

The risk management is primarily concerned with the "management" of information according to Erben and Romeike [21]. The decentralism of grown structures in the context of IT risk management ensures that relevant data in different ranges of the enterprise is available, but that it is deficient in a coordinated collection, storage, manipulation and provisioning [21]. The major task of a risk management information system (RMIS) is to provide operation- and decision-makers with essential and relevant information in an economically useful way [21].

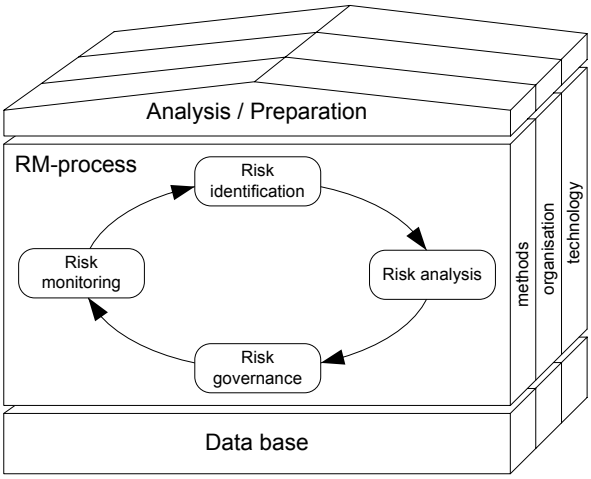

Figure 3. Architecture risk management information system

The main aim of RMIS can be described as the support of the overall risk management process [20]. The governance of this process requires the support of analysis- and preparation outputs [21]. For the support essential data has to be provided centrally, which is obtained e.g. from operating systems or external information sources [3, 21]. By realizing a process-oriented design of decision support systems, apart from the integrated perspective of the process view the view

of methodical designing, organizational aspects and technical realization has to be explicitly taken into account [20]. An illustration of this model by architecture is shown in figure 3.

A RMIS must be methodically, organizational and technically linked with the requirements of the risk management process. On the one hand standard methods must be provides for each step like e. g. fault tree analyses for the compilation or risk matrixes at the analysis level. [21]. On the other hand it is important that the substantial reference models are supported like the IT Baseline Protection Manuel, *Information Technology Infrastructure Library* (ITIL) or the *Control Objectives for Information and Related Technology* (CobiT), which usually refers to the IT Security Management or IT System Management. The organizational networking of various participants in the IT Risk Management requires e.g. that event-driven communication mechanisms are assured by modern electronic communication systems. [12, 21, 22]. Technical aspects concern e.g. the binding to the operative systems e.g. like Business Impact management solutions [23], as a promising means in this context. In addition also external databases must be integrated into the RMIS as information sources, analogous to the integration of information sources into a data warehouse. [3, 21]. Further aspects are the binding to analytical systems or the complete embedding into the IT infrastructure [21].

3. Requirement analysis and empirical investigation

3.1. Developing requirement criteria

On basis of the introduced framework for RMIS a set of criteria for the analysis of requirements for application systems can be derived. For this purpose requirements for the design of RMIS will be seperated analogous to the outlined framework in the areas of ‘processes’, ‘methods’, ‘analysis and conditioning’, ‘organization’, ‘technology’ and ‘preface’. Subsequent, based on these criteria, for a variety of application systems for the ORM their suitability for the IT-risk management is examined. The set of criteria with exemplary requirements is shown in figure 4.

Due the fact that risk management is to be seen as a holistic process it is necessary that a RMIS can offer an adequate support in all phases of the risk management process [21]. Therefore one criterion is to examine which steps of the process are supported. Furthermore it is important to point out how the individual phases in the RMIS are supported. The presence of e.g. standard risk lists or semi-structured questionnaires for the identification and assessment of risks [24]. Furthermore it should be assessed how far these are integrated over the whole process respectively, i.e. whether measures are directly assigned to different risk types. In practice of the IT Security- and system management in particular for the IT Security Management numerous of standards and "Best Practices” have been established. These standards offer an extensive improvement in efficiency at the accomplishment of the IT Risk management. Another essential requirement is the support of IT Basline Manual, ITIL and CobiT or the possibility to implement support by hands.

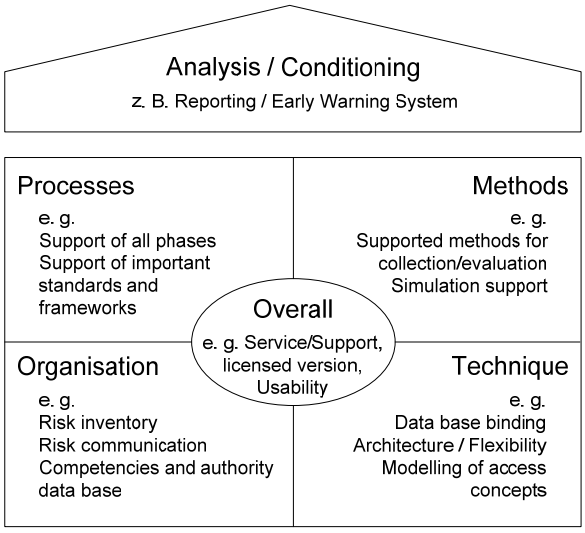

Figure 4. Set of criteria for the investigation of RMIS

The intention-compliant support of the risk management by a RMIS particularly depends on the dimension of the support of the necessary methods for instrumental arrangement by the software [22]. In addition, following the method overview of Romeike & Erben, it will be proved which methods are offered for the risk identification and evaluation by the software [21]. Thereby, special emphasis has to be placed on the large support from simulation methods, which allow to asses several complex application scenarios in order to reduce the effect and evaluation defects [21] or to aggregate single risks (e.g. by Monte Carlo Simulations) to a total risk extent [25].

For a meaningful support of the risk management software components that enable an aggregation and a

clear representation of necessary information is essential [21]. Therefore in the area of "analysis/conditioning" it has to be examined if reporting systems with standardized and individual reports are offered [22]. Hence it is important, with which presentation and visualization possibilities (e.g. clear tables, Portfolios, diagrams) the data can be prepared in accordance to the target audit. In addition the suitability of the RMIS as early warning system has to be examined. In order to be able to anticipate prospective developments and events and to control suitable preventive measures, the software has to offer indicators or characteristic numbers for the monitoring of risks [21]. Another requirement for a warning system is, to monitor critical levels. Besides this it needs to be examined in how far the pre-defined indicators are extensible.

Among the support of the risk management process the organizational structure of the risk management must be supported, too. This applies in particular in the context of IT risks because functions with regard to the co-ordination of IT safety precautions approaches and to the central IT Risk management should be integrative. A central risk inventory is a substantial demand, in order to assign and prioritize measures for certain risks [21, 22]. Thus it has to be examined to what extent the risk management system permits to bundle decentralized existing knowledge and to avoid risks range-spreading [21]; [22]. A further requirement, which results from it, is the support of communication among the involved participants [21]). Besides it has to be examined to what extent the system allows the illustration of organizational structures, appropriate function carriers and their competencies. A further criterion is the allocation from qualifications to the actors.

Since it is necessary for spreading view to be able to access an integrated volume of data [21], the data base support represents a particularly important technical aspect [24]. For the resuming analyses RMIS should offer methods such as OLAP or DATA Mining or support the use of appropriate tools [22]. Regarding the architecture particularly the question of integrating ability into the IT landscape of the enterprise is important. Here e.g. it needs to be examined whether interfaces to other components of the operational information system (e.g. to the operational account system) [21] or the project planning tools [24] are offered. An essential requirement for the use of external sources is the presence of data import and export functionalities [22]. Other requirements include the scaling bar and the ability of customizing [22]. In order to support setting of tasks according to teams over several organizational units, network ability and the support of web surfaces are necessary. Further criteria focus on the supported platforms and the possibilities for the right support and user administration to illustrate the organizational role concept adequately.

With the criteria of the range "Overall" it is finally assessed, which service and support respectively a manufacturer offers e.g. regarding a detailed documentation (e.g. in the form of on-line assistance), training courses or a current user support (help desk) of a risk management software [22, 25]. Secondary further aspects like the update politics, the license model and the usability incorporate.

3.2. Survey design

Operational Risk management and information security management having been developed in practice largely isolated, as well as the corresponding application systems. Therefore it needs to be evaluated, in which way the software artifacts for ORM, available at the market, offer enough functionality to support IT-Risk management. 31 different Systems have been identified at the German market. Systems that neither focus on operational risks in general, nor specially on

Product	Company
Focus ORM	
c.-RiskManager	Cederos
MIS Risk Management	MIS
OpRisk Suite	RCS AG
procora	focus consulting & services AG
ProKoRisk	ifb group
R2C_risk to chance	Schleupen AG
rimanis	Hulocon
RiskDecision	Incom / noweco
Risk Dimensions	SAS
Risk Scout	IDS Scheer
RiskCity	Decisio
RISKIT	Astrum
RISKMANAGER	Corporate Planning
RiskManager	COR GmbH
RiskReporter	BMS Consulting GmbH
Focus ISM	
CRISAM Explorer	calpana business consulting gmbh
GSTOOL	BSI

Figure 5. Chart of the inquired Systems

IT-Risks are not included in the sample. These systems include for example systems, that are only dealing with financial risks (e.g. "Algo OpVar"), or systems, which just offer part-time solutions to Risk management, like simulation-tools e.g. "@RISK" and "Crystal Ball". Furthermore systems have been excluded, where not sufficient information could be gathered within the period of inquiry. The Applications, included in the inquiry, are displayed in figure 5.

The criteria of the presented general-framework were converted in an evaluation sheet, to make the inquiry operable. Thus the remaining 17 systems were assessed on that basis. This approach allows a structured assessment and safeguards a high level of comparability.

3.3. Brief presentation of the results

Based on the catalogue of criteria formulated before, the 17 named applications were assesd with regard to their suitability for the IT-Risk management. Every system was analyzed and evaluated by the criteria of *Processes, Methods, Analysis and Processing, Organization* and *Technique/Technology*. The inquiry conclusions are summarized briefly in the following.

In the field *"Processes"*, nearly none of the systems is able to fulfill the requirement of supporting all tasks in IT-Risk management. The majority of the systems support the procedure according to the general risk process. Mostly the general rules of reference models are not integrated by default, but can be converted manually. The GS-Tool and the CRISAM Explorer are exceptions, where, corresponding to the CRISAM-method, all inquired standards are supported [26]. In the field of *methodical support*, just a third of the systems are able to fulfill all criteria completely. While three quarters of the inquired systems fulfill at least the criteria of method support, regarding the identification and valuation of risks, simulation support is offered only by one third.

In the field of *"Analysis and Processing"*, all systems fulfill at least the reporting criteria partially, even over two thirds completely. Though only one half offers enough functionality to apply them as an early-warning system. In contrast to that, the organizational demands are fulfilled by nearly all risk management systems. While the management of risk inventories and the responsibility maintenance is extensively fulfilled by every system, the field of supporting the risk communication should be developed further. In term of *technological* criteria it could be ascertained, that the demands to the users administration are predominantly fulfilled. The fields of architecture and data base support, referring to the set of criteria, are only fulfilled by one third completely, one half fulfilled at least in some cases.

4. Summary and Outlook

Even if the demand for a successfully operating IT-risk management can hardly be derived from the corresponding regulations, the economic ratio and the expectation of additional, tightened norms requires to run a company-wide operational risks management that comprises IT-risks adequately [7]. Furthermore the company-wide operational risk management needs to be integrated in a way that the possible synergy-effects can be realized. The organization of such an IT-risk management is archetypal described in this article. It can be stated that this is only possible with the support of an adequate risk management-information system. A general-framework was presented, which allows a derivation of a criteria catalogue for assessing available software systems. Afterwards 17 software systems available at the German market tested have been assessed on that basis.

The analysis displays that there are no systems available yet supporting an integrated IT-risk- and -security management. A partial support can be achieved by two types of systems: on the one hand side applications for the ORM, on the other hand side, modeling tools for entrepreneurial information security management. There might be RMIS existing, which handle in general with the management of operational risks, but these systems are not tailored for IT-risk management. In addition, there are tools, which could be used for modeling and therefore support an adaption of the information security management for a specific company. These tools offer, for example, support by the planning of measures by suggesting specific (reference-) measures for a modeled target and by helping to identify (reference-) threats for the target.

By focusing on classical information security or operational risk management, important aspects of an integrated IT-risk management are disregarded. Suitable applications for the IT-risk management though are not short-term expectable, because there is even a need for a method-development to support an IT-risk management. The research in this field should be targeted to practical applications. There are some preliminary works that should be extended in the

future. A first approach is for example to offer reference-models like the BSI Baseline Manual supporting an integration of information security management in existing solutions for ORM. Further potential is seen in the linkage to business impact solutions. If those potentials are realized application systems for ISM offer the opportunity by the enrichment of specific functionalities, to become full solutions for an IT-risk management. Therefore future work should focus on the design of systems that enable a convergence of ORM and ISM. In the conceptual design of such systems the identified criteria should be taken into account.

References

[1] H. Krcmar, *Informationsmanagement*. Heidelberg, 2003.

[2] T. Neubauer, M. Klemen, and S. Biffl, "Business process-based valuation of IT-security," in *Seventh international workshop on Economics-driven software engineering research*, St. Louis, 2005, pp. 1- 5.

[3] M. Falk and M. Hofmann, "Integration des IT-Sicherheitsmanagements in das Risikomanagement im Kontext bankaufsichtsrechtlicher Vorgaben. Arbeitspapiere Wirtschaftsinformatik," Justus-Liebig-Universität Gießen, Gießen 2006.

[4] J. A. Hall and S. L. Liedthka, "The Sarbanes-Oxley Act: Implications for Large-Scale IT-Outsourcing," *Communications of the ACM,* vol. 50, pp. 95-102, 2007.

[5] J. A. Hall, "The Sarbanes-Oxley Act: Implications for Large-Scale IT-Outsourcing," in *Communications of the ACM*, 2007.

[6] L. Lensdorf and U. Steger, "IT-Compliance im Unternehmen," 2006.

[7] M. Klotz, "Basel II als Treiber des IT-Sicherheitsmanagements - eine Klarstellung," 2007.

[8] B. A. f. B. BAB, "Die Neue Basler Eigenkapitalvereinbarung – Konsultationspapier in Übersetzung der Deutschen Bundesbank," 2001.

[9] K.-R. Müller, *IT-Sicherheit mit System. Strategie – Vorgehensmodell – Prozessorientierung – Sicherheitspyramide*. Wiesbaden.

[10] H. Seibold, *It-Risikomanagement*. München, 2006.

[11] H.-P. Nägeli, "Management der Informationssicherheit – Erfahrungen eines Finanzdiensteleisters," Heidelberg 2003.

[12] H.-P. Königs, *IT-Risiko-Management mit System. Von den Grundlagen bis zur Realisierung – Ein praxisorientierter Leitfaden*. Wiesbaden, 2005.

[13] K. Schmidt, *Der IR Security Manager*. München, 2006.

[14] C. Locher, "Integrative Managementkonzepte für operationelle Risiken: Integration von operationellem Risikomanagement und IV-Sicherheitsmanagement," Weinheim 2005.

[15] T. Mai, *Management der Organisation. Organisation der Sicherheit*. München, 2003.

[16] P. Konrad, "Geschäftsprozeßorientierte Simulation der Informationssicherheit: Entwicklung und empirische Evaluation eines Systems zur Unterstützung des Sicherheitsmanagements," Köln, 1998.

[17] S. Sitzberger and T. Nowey, "Lernen vom Business Engineering - Ansätze für ein systematisches, modellgestütztes Vorgehensmodell zum Sicherheitsmanagement," in *Multikonferenz Wirtschaftsinformatik 2006*, Berlin, 2006, pp. 155-165.

[18] S. Röhrig, "Using Process Models to Analyse IT Security Requirements," Zürich, 2003.

[19] S. Jakoubi, S. Tjoa, and G. Quirchmayr, "Rope: A Methodology for Enabling the Risk-Aware Modelling and Simulation of Business Processes," in *Fifteenth European Conference on Information Systems*, St. Gallen, 2007, pp. 1596-1607.

[20] J. vom Brocke, *Referenzmodellierung, Gestaltung und Verteilung von Konstruktionsprozessen*. Berlin: Logos Verlag, 2003.

[21] R. F. Erben and F. Romeike, *Risk-Management-Informationssysteme – Potentiale einer umfassenden IT-Unterstützung des Risk Managements*, 2007.

[22] A. Jonen, Lingnau, V., Schmidt, T., *Lynkeus - Kritischer Vergleich softwarebasierter Informationssysteme zur Unterstützung des Risikowirtschaftsprozesses*, 2006.

[23] M. Hofmann, *Management operatationaler IT-Risiken im Kontext von Basel II, MaRisk und anderen aufsichtsrechtlichen Vorgaben*. Hamburg, 2006.

[24] H. Reckert, "Lösungsansätze zum Risikomanagement," Berlin, Heidelberg 2003.

[25] W. R. Gleisner, F., "Anforderungen an die Softwareunterstützung für das Risikomanagement," 2005.

[26] C. B. C. CBC, *CRISAM. Risk Management*, 2006.