December 2004

A Framework for Classifying the Operational Risks of Outsourcing - Integrating Risks from Systems, Processes, People and External Events within the Banking Industry

Heiko Gewald
Johann Wolfgang Goethe-University

Daniel Hinz
Johann Wolfgang Goethe-University

A Framework for Classifying the Operational Risks of Outsourcing

Integrating Risks from Systems, Processes, People and External Events within the Banking Industry

Heiko Gewald

E-Finance Lab
Institute for Information Systems
Johann Wolfgang Goethe-University
Frankfurt am Main, Germany
gewald@wiwi.uni-frankfurt.de

Daniel Hinz

E-Finance Lab
Institute for Information Systems
Johann Wolfgang Goethe-University
Frankfurt am Main, Germany
dhinz@wiwi.uni-frankfurt.de

Abstract

Operational risk and outsourcing are two major topics on today's agenda of top executives, especially in the banking industry. This paper introduces a framework to classify operational risk in outsourcing in a way that generates quantifiable output for measurement purposes. The authors developed a matrix system that deploys a catalogue of sources of risk and a mutually exclusive yet exhaustive system of measurable impact areas. It is shown that this framework adds to the understanding of operational risk as its application enhances transparency through the transformation of often vague risk descriptions to quantifiable risk indicators. An overview of the current IS literature on risks in outsourcing combined with a critical assessments of deficiencies for transparent risk classification serves as a input for the classification process.

Keywords: Outsourcing, Operational Risk, Banking, Classification Framework

1. Introduction

„These days, the business of banking is risk management."
Dennis Westherstone
Retired JP Morgan chairman

Operational risk and outsourcing are two major topics on today's agenda of top executives, especially in the banking industry. The reasons for this are various like:

- **Cost pressure**
  Declining margins, extended competition, and unfavourable stock exchanges lead to cost containment measures. During the years outsourcing has gained a reputation as being a suitable management instrument to save costs.
- **Technological innovation**
  The banking industry has changed dramatically over the last 20 years. To a large part this is due to the electronic revolution of the internet and its impact on B2B and B2C relationships. The downturn of this is the dramatic increase in technological complexity of the bank's operations.
- **External events of a new dimension**
  After the terrorist attacks of 9/11 the worst case scenarios for external events have dramatically changed. The common scenario of losing a production facility (e.g. a

data processing centre) has to be replaced by contingency plans for the inaccessibility of a whole financial centre [Federal Reserve Bank of New York 2002].

- **New regulatory laws**
  The anticipated New Basel Capital Accord requires banks to support their operational risk with equity capital, a scarce resource.

These four points are intentionally mixed up between being drivers for operational risk and outsourcing or both. This is to show how closely both topics interact. Within this paper a framework will be developed that helps to classify the operational risks of outsourcing to increase transparency in the process of mitigating them.
We believe that operational risk in outsourcing needs to be a domain of the IS community (see call for papers of AMCIS 2004). As the role of the CIO changed over time from delivering bits and bytes to delivering value it is important not only to understand the business of the users but also to have an understanding of the risks inherent in the underlying operations. The IS community has adopted outsourcing as its domain and already discussed the risks involved under different motivations (see e.g. the outsourcing minitrack at HICSS over the last years). The next logical step would be to shift focus from assessing the risk within the outsourcing decision to understand and manage the risks inherent in delivering outsourcing services.
This paper starts with a characterization of the terminology employed and a brief description of the theoretical and practical motivation. The following section provides an overview of the IS literature on risks in outsourcing combined with a critical assessments of shortcomings for transparent risk classification. Building on these insights, we introduce a classification framework to decompose operational risk in outsourcing in a way that enables the corporate risk management function to measure it consistently on corporate level. Furthermore we propose the deployment of Bayesian Belief Networks to simulate the outcomes of changes in the risk structure through outsourcing. The final section provides the conclusion and an outlook for further research.

2. Operational risk and outsourcing

This paper addresses the operational risks inherent in outsourcing operations of financial institutions specifically in the banking industry. To ensure a common level of understanding, we start with a series of definitions and explanations of the most important terms before we refer to the practical and theoretical motivation of our work.

2.1. Characterization of terminology

2.1.1. The New Basel Capital Accord

The Basel Committee on Banking Supervision, a committee of the Bank for International Settlement (BIS) located in Basel, Switzerland is the highest international body for banking supervision. Regulations by the committee are not legally binding to the member states, nevertheless the formulated standards are usually translated into national regulation to ensure consistency in the global banking system (for further information see www.bis.org).
In 1988 the Committee decided to introduce a capital measurement system known as the Basel Capital Accord (commonly referred to as "Basel I") for the mitigation of credit risk. Since then this framework has been progressively introduced not only in member countries but also in virtually all other countries with active international banks. In June 1999 the Committee issued a proposal for a New Capital Accord ("Basel II") to replace the 1988 Accord. One of the new challenges of Basel II is the necessity to measure operational risk and to include the results into the capital measurement system [Basel Committee on Banking Supervision 2003]. The current due date for the implementation of Basel II is 2006.

2.1.2. Risk

The implications of risk have been examined in several domains of the scientific literature for many years (early articles date back to the 1920s [Knight 1971]). As the topic has been discussed in both great detail and extensive breadth, several definitions emerged every one of them tailored for a specific demand (overviews from different perspectives are given in [Pfleeger 2000], [Aubert et al. 2002], [Renn 2004]).

In this paper we focus on risk in the banking industry and for this purpose adopt a definition of risk which has already been introduced within the finance domain and therefore is compatible with existing risk management concepts. We use the definition of Jorion and Khoury: "Risk can be defined as the volatility of unexpected outcomes" [Jorion and Khoury 1996] as a basis and extend it to make it more precise: *Risk is the measurable probability of the negative deviation of a target value from a reference value*. Note that risk is different from uncertainty, which is not measurable.

2.1.3. Operational risk

Various authors have discussed the issue of operational risk and worked out respective definitions (for a comparison of different approaches see [Netter and Poulsen 2003] or [Goodhart 2001]) but a commonly accepted definition has not yet been developed. Many authors draw on the Basel Committee for a starting point which defines operational risk as the *risk of loss resulting from inadequate or failed processes, people and systems or from external events* [Basel Committee on Banking Supervision 2003]. In the following we will use this definition if we refer to operational risk.

The other major sources of risk in banking are engagements in the market (i.e. volatility of market prices, exchange rates, interest rates etc. = market risk) or in credits (i.e. a debtor not paying back a loan etc. = credit risk). Those will not be reflected in this paper (an in depth discussion of these risks is given in [Jorion 1996]).

2.1.4. Risk management process

The process of risk management, sometimes also referred to as a risk management framework, has been discussed by a number of authors (for an overview see [McConnell and Blacker 1999]). Although the terminology often differs slightly a common basis can be found built around four phases:

1. **Identification**
   Systematically recognizing sources of risk
2. **Measurement**
   Estimating probabilities, severities etc. to quantify risk
3. **Management**
   Decide on an appropriate course of action to handle risk
4. **Control**
   Back-test the success of measures taken to mitigate risk

The aim of the risk management process is to adequately handle all risks a bank faces. It is applied to all types of risk (market, credit and operational risk) and ideally consolidates risk management techniques and practices as well as actions to mitigate risk on a corporate level.

As this paper introduces a classification framework, we will focus on the identification phase of the process. Nevertheless it is important to keep the following phases in mind, as the output of the identification phase feeds in as input for the measurement phase.

2.1.5. Outsourcing categories

Within this paper we will take a broad view on the operational risks associated with outsourcing not limited to IT infrastructure outsourcing (ITO) but also incorporating Application Service Providing (ASP) and Business Process Outsourcing (BPO). Therefore, we firstly define the term outsourcing in general, followed by a definition of its associated three categories: ITO, ASP and BPO.

Outsourcing

As this paper focuses on the banking industry, we will use a definition of outsourcing as incorporated in several European regulatory laws (an overview on alternative definitions is given in [Gilley and Rasheed 2000] or [Dibbern et al. 2004]). Our definition is based on the description of the Deutsche Bundesbank as given in its circular regarding the outsourcing activities for banks conducting business in Germany [Deutsche Bundesbank 2001]. *An outsourcing occurs whenever an institution (customer) commissions an external enterprise (service provider) to perform, permanently or at least for a prolonged period, an activity or function (service) that is essential to the customer's business.* This definition covers different types of outsourcing, hereafter referred to as "outsourcing categories". Those are defined as follows:

IT Infrastructure Outsourcing (ITO)

In analogy to Earl's definition of information services outsourcing [Earl 1991], ITO will be defined as *outsourcing hardware-orientated IT activities such as data centre operations.* This definition includes a variety of activities like user helpdesk services, network management etc.

Application Service Providing (ASP)

Based on the definition of the CompTIA Software Services Group (formerly known as the Application Service Provider Industry Consortium - ASPIC), ASP will be defined as managing and delivering application capabilities to multiple entities from a data centre across a wide area network.

Business Process Outsourcing (BPO)

BPO will be defined as outsourcing one or more specific business processes together with the IT that supports them [Halvey and Melby 2000], where a business process is defined to be a set of logically related tasks performed to achieve a defined business outcome [Davenport and Short 1990].

2.1.6. Outsourcing process

On a very high level the process of outsourcing can be separated into four main phases.
During (1) the *pre-deal phase* the decision whether to outsource or not will be reached. Using tools and techniques like business case calculation, core competency examination, critical success factor analysis etc. the corporation assesses the potential gains and drawbacks from outsourcing, finally answering the question if and what to outsource. (2) the *contractual phase*, which comprises the vendor selection process and the contract negotiation. Within this phase, the outsourcing object needs to be specified in sufficient detail, including service level agreements etc. (3) the *transition phase*, in which processes, systems, and probably people are handed over from customer to service provider. This phase has typically the status of a project. (4) the *delivery phase*, in which the business will be provided from outside resources. This phase actually becomes a steady state for the time the outsourcing engagement lasts.

2.2. Practical and theoretical motivation

The three outsourcing categories described differ in their level of maturity within the outsourcing community. ITO dates back to the early 1960s and gained momentum through the 70s and 80s (for a historic review see [Hirschheim and Dibbern 2002]). To the current date a significant number of deals with an enormous contract value has been closed [Caldwell 2003] and the topic has been intensively discussed in scientific literature (for an in depth overview see [Gilley and Rasheed 2000]). During the late 1990s the ASP business model emerged (see e.g. [Stambaugh 1996]) and is still in the process to find its economic base (see e.g. [Kern et al. 2002]). Scientific literature has covered this topic lately, especially from the early 2000s [Susaria et al. 2003]. BPO is a relatively new outsourcing arrangement [Hirschheim and Dibbern 2002], to date hardly covered in scientific literature and on the practical side still comparatively infant but with large growth expectations [Lukacs et al. 2002].

The maturity levels described are also reflected in the "IT Value Chain" as described in [Cross et al. 1997]. In this paper the emphasis to outsource was top ranked for infrastructure, followed by applications, information, and business processes. Taking a look back through the last decade this is what happened in practice for a broad set of industries [Kakabadse and Kakabadse 2002].

Within the banking industry all three categories of outsourcing are used. However, a transparent framework for classifying the operational risks inherent in employing outsourcing services is, to the best of our knowledge, currently missing. This paper aims to bridge this gap through providing a framework that enables the corporation to transparently measure the associated risks.

From a theoretical perspective we analyze the current IS literature on risks in outsourcing and map the results on a matrix displaying the sources of operational risk and their dedicated impact areas (the parameters hit if a loss occurs). Contrary to the majority of the existing literature we focus our analysis on the delivery phase of the outsourcing engagement, not on the pre-deal or contractual phase. The delivery phase is of special interest, as this is the phase where operational risk usually occurs, the risks in the preceding phases are mainly strategic risks.

3. Risks as Identified in Current IS Literature

3.1. Overview of the literature

Current IS literature has discussed outsourcing and its benefits and risks in great detail. The following overview is focused on literature with a distinctive concentration on outsourcing risk, leaving standard outsourcing literature untouched (for an overview see [Dibbern et al. 2004]). Note that current literature often mixes one-time risks during the pre-deal and the contractual phase with recurring operational risks in the delivery phase. In this section we will discuss a brief overview of the analysed sources, a detailed listing of the identified references and risks discussed in there is given in the appendix.

Aubert et al. provide a holistic view on the dangers of IT outsourcing covering the transition process and operational aspects after the transition [Aubert et al. 1999]. Seven "undesirable outcomes" have been extracted from current literature, for example unexpected transition and management costs, service debasement, and loss of organizational competencies. An even wider approach is taken by Earl including also the general issues of information systems, e.g. endemic uncertainty [Earl 1991]. A decision-oriented assessment with ten risk factors is provided by Willcocks et al. who include also unrealistic expectations and inadequate outsourcing goals like cash injection [Willcocks et al. 1999]. Alexander et al. reduce the risks to six main risk types including e.g. impact on staff morale, but leaving out skill aspects, which are regarded as important by other authors. Lacity names cost overruns, declining service levels,

and lack of innovation as the major defects identified by an empirical study [Lacity 2002]. According to Ang and Toh the greatest risk of outsourcing is the loss of control ([Ang and Toh 1998]). Adeleye et al. put their focus on the contractual phase by referencing deadline overrun and deficient change over [Adeleye et al. 2004]. Jurison identifies 13 individual risks, considering risks not mentioned within the other sources, like lack of trust [Jurison 1998].

3.2. A critical review

Current literature has not only discussed the benefits and promises of outsourcing, but the downsides in detail as well. Most of the identified risks shown above have been derived from case studies and provide a broad basis for identifying the risks of outsourcing. They are well suited to give both academics and practitioners a comprehensive impression of possible defects when employing outsourcing services. Nevertheless this explorative approach has to face the criticism, in how far these risks fit in a structured framework. At least the diversity of the different risk listings might induce some scepticism. Another challenge arises from definitions of risk which focus on the aspect of measurability: Current literature often lacks a rigid definition of risk and mixes risk with uncertainty, for example hidden costs is a measurable risk, while supplier dependency can neither be measured nor has it necessarily directly negative implications. Also literature tends to not differentiate the risks of the different phases of the outsourcing process, for example unexpected transition costs are related to the contractual phase, while unexpected management costs are mainly related to the delivery phase. This has a strong influence on the decision process whether to outsource or not, as the risk mitigation strategies and the risk transfer is different, depending on the particular phase.

4. The Classification Framework

4.1. Overview of the model

The review of the literature on the risks of outsourcing gives a good indication on what risks are associated to the decision to outsource part of the corporate functions. To support the decision process a scenario analysis comparing the current risk structure and the future risks structure after outsourcing would give valuable insights.

Our proposed model is based on a structured decomposition of the identified risks, by employing a matrix system which maps the sources of risk to areas where losses resulting from those risk become apparent, the so called impact areas. Sources of risk are broken down to key risk drivers (KRD), which are mapped to their corresponding key risk indicators (KRI) on the impact area axis. If there is a cause-effect relationship between a KRD and a KRI a risk indicator (RI) will be assigned to the intersection within the matrix. This RI has to be quantifiable to enable the measurement of the overall risk profile.

4.2. Measurement driven classification

The collection of risks as described in section 3 lacks some important characteristics to be used for risk measurement purposes, the second phase of the risk management process. To assess the level of operational risk and its composition it is crucial, that the identified risks fulfil three main criteria.

First of all, they have to be *measurable* to allow for a quantitative assessment ensuring the consolidation of these risks with other risk types within the bank to gain a complete overview of the corporate risk position. Secondly, they have to be *mutually exclusive,* so that double-counting is avoided as otherwise the calculated risk measure would be overstating the risk position. Thirdly, the risks have to be *completely exhaustive* so that no relevant risks are missing in the assessment. A violation of this criterion would result in a risk assessment underestimating the banks risk position.

The aim of this paper is to develop a framework that classifies the identified risks in a way that ensures coherence with the stated criteria. To confirm this we employ a simple insight as a basis for our framework. We see that every risk has a source where it originates and an impact area where it materializes. To ensure consistency with the criteria stated above, we developed a matrix system that integrates a comprehensive catalogue of sources of risk on the ordinate and mutually exclusive yet exhaustive system of measurable impact areas on the abscissa. The risks as given in the section above will be assessed in a transparent manner through applying the framework, i.e. decomposing them on the matrix by assigning sources and identifying impact areas.

4.3. Sources of risk

The definition of operational risk as used in this paper, which is the definition of Basel II, focuses on four sources of operational risk: processes, systems, people and external events.
These sources need to be classified for the sake of ability to control them. They are either endogenous or exogenous, meaning controllable by the organisation or not. A natural disaster like an earthquake for example is exogenous, as the occurrence of it cannot be influenced by the bank (a description of this concept is given in [Aubert et al. 2002]). Following this thought, external events are classified as exogenous, while risk resulting from processes, systems and people is endogenous.
This distinction is important as within our framework we regard the outsourcing engagement as endogenous, meaning the risk resulting from processes, systems and people is controllable by the parties involved in the outsourcing engagement (customer and service provider), therefore the service provider is not to bee seen as external in this context and therefore defects resulting from the service provider are not exogenous. This thesis is supported by regulatory laws in several countries, which argue that a bank has to be in charge of its operations regardless if outsourcing services are used or not. The sole treatment of the service provider as a black box with defined input and output interface is not acceptable (see e.g. [Deutsche Bundesbank 2001]).
We chose to nominate the risks given in the definition of operational risk as basic classification for the sources of risk, as they could be regarded as exhaustive. Every risk occurring could be classified as either originating from processes, systems, people or external events.

- **Processes**
  This source of risk incorporates all processes that interact with the outsourcing engagement, may this be business processes (especially in BPO), administrative / support processes like software changes in ITO or the requirements management processes in case of ASP.
- **Systems**
  The term *systems* incorporates all information technology and communication systems, including hardware and software. It accounts for PCs, mainframes, telecommunication etc.
- **People**
  This source of risk covers all people and organisational related matters. In outsourcing engagements typically governance, know-how, and principal-agent questions have to be considered.
- **External Events**
  As laid out before, external events cover the exogenous part of operational risk, typically natural disasters, terrorist attacks, and political risk (e.g. the disseizin of corporate property).

The sources of risk can be further refined into key risk drivers (KRDs), a KRD being a quantifiable and manageable portion of its superior source of risk. These attributes are important

due to the fact that in the process of modelling the assessed risk they play the role of an anchor point which management needs to address with action if a risk should be influenced in a specific direction. An example in the source *information systems* is the KRD *systems reliability*.

4.4. Impact Areas

Regulatory approaches like Basel II and the majority of the financial risk management literature favour cost as the only figure to quantify possible impacts. Concerning Basel II this arises from the aim to determine a capital charge, but also practitioners and scientists tend to prefer quantitative monetary approaches over qualitative ones [Pfleeger 2000]. As a (reduced) capital charge is the only real incentive a regulator can provide to encourage banks to enhance their operational risk management [Herring 2002], it has to be critically reflected if monetary quantification is the correct way to achieve this goal (see e.g. [Brink 2003], [Goodhart 2001]). The discussion whether purely financial indicators should be employed is two-fold. On the one hand the impact of a risk should be expressible in cardinal numbers with costs being the natural choice, otherwise there can be neither a comparison of different risks regarding their magnitude, nor can the relative effectiveness of different mitigation levers be assessed. On the other hand the rigorous focus on costs assumes financial targets as the governing objective of a firm and widely neglects other objectives like e.g. quality leadership. To support a more diverse assessment we introduce a set of areas that are affected by losses resulting from operational risks, so called impact areas.

Simple yet compelling operational performance measures are offered by the three dimensions cost, time, and quality typically used in product development, project management, and manufacturing, as all three dimensions are measurable [Tatikonda and Montoya-Weiss 2001].

A review of the literature indicates that the most often cited impact area in outsourcing is *cost* (see e.g. [Alexander and Young 1996], [Jurison 1998]). This may be due to the fact, that most outsourcing decisions have a focus on cost cutting [McLellan et al. 1995], and missing the cost reduction target would negate the deal benefits.

Another often quoted risk is supplier dependence (see e.g. [Alexander and Young 1996]). Although not a negative issue per se, lock-in situations could be leveraged by providers to increase prices or provide lower-quality services. This argument supports our second impact area: *quality*. This issue has also been referred to as service debasement [Aubert et al. 1999].

Time losses are not explicitly pointed out as outsourcing risks but are inherent in other risks like service debasement [Aubert et al. 1999], and a prolonged time-to-market of innovations [Lacity 2002] due to loss of skills [Jurison 1998].

Although quality is a qualitative measure, it is still relatively easy to assign quantitative figures to it e.g. by applying scoring models. Concerning exclusiveness it is important to realise that these three parameters are naturally depended, e.g. quality issues can have effects on costs, time lags might have effects on quality and costs. Therefore it is crucial to distinguish between cause and effect and clearly allocate a risk either to only one impact area or to split it up between multiply impact areas to avoid double-counting. Note, that in the same way a risk can have more than one source it can have more than one impact area. Thirdly, these areas are in so far completely exhaustive, that in case a risk cannot be assigned to one or the other impact area, the effects of this risk could be translated to monetary figures and be applied to the cost area.

Impact areas are further refined into key risk indicators (KRIs), which represent parameters of the impact areas that allow for condensed communication to senior management. An example for the impact area *quality* is the KRI *failed transactions*.

4.5. The classification framework

The combination of the sources of risk (section 4.3) and the identified impact areas (section 4.4) leads to a matrix as depicted 如下 which will be utilized during expert workshops, when assessing the operational risks of outsourcing.

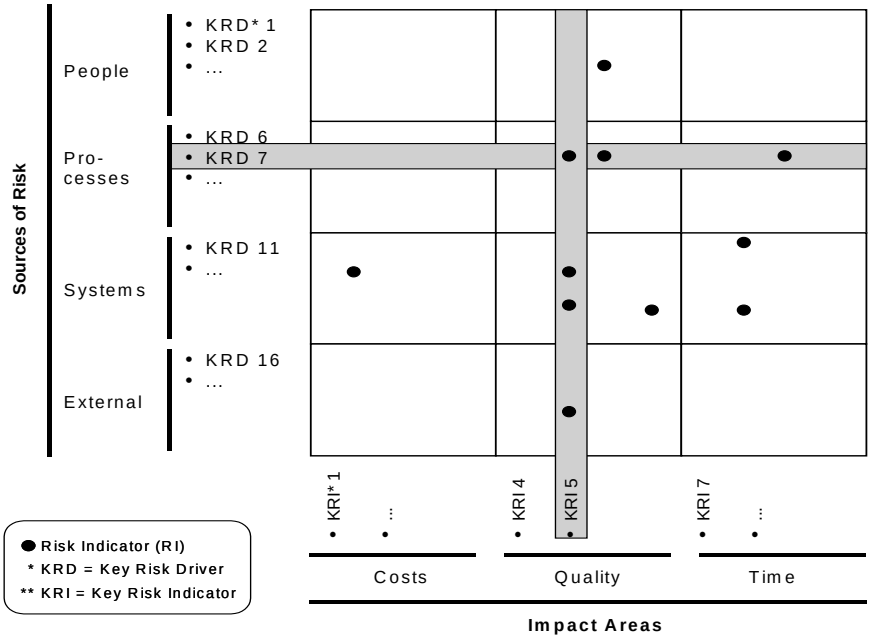

Figure 1: The Classification Matrix

The left hand side of the matrix lists the sources of risk, acting as the logical starting point for the classification process. Every risk to be assessed using the framework needs to be assigned to a KRD in the first instance (note that it is possible to assign more than one source to a risk). The abscissa of the matrix lists KRIs of the impact areas. After the sources of risk have been identified impact areas need to be applied, which will be done by assessing the areas that are affected if the risk (which is per definition just a probability) becomes a loss (which is certain). A loss in this context can be measured in either monetary terms, a decline of quality or an increase in time needed to fulfil a task. A risk can be applied to more than one KRI.

The segregation of a specific risk into its KRDs and KRIs leads to intersections. Every intersection represents a need to measure risk, which will be done by assigning at least one risk indicator (RI) to them. A RI is a quantifiable measure which represents its fundamental KRD and the affected KRI. RIs need to be assessed either automatically (as part of service level agreements) or through periodic expert assessments.

To decompose the risks of outsourcing and to identify the relevant RIs expert workshops have to be conducted. These workshops fulfil three objectives, firstly experts have to identify potential additional risks of a specific outsourcing situation not covered in literature (which serves as a starting point), secondly they have to decompose the risks and to identify dependencies, and thirdly they have to estimate individual probabilities where statistical data is not available or scarce. Expert workshops usually provide sufficient data to fully specify risk information, but special attention has to be paid to quality issues as expert data is usually biased [Ebnöther et al. 2002].

In this way the operational risks of outsourcing can be decomposed. Additionally, the results from internal audit reports or additional expert advice can be assessed in the same manner.

4.6. Indicative validation

This model represents a fundamental building block of a larger research project on the management of operational risk in outsourcing. The ultimate goal is to provide a theoretically founded method that enables decision makers to assess the operational risks inherent in the outsourcing decision more thoroughly than currently possible. We aim to achieve this goal by modelling the relationship of cause and effect between KRD, RI, and KRI with a transformation into a Bayesian Belief Network. This will be the underlying method for a risk scorecard, serving as a decision support tool to conduct scenario analyses on the risk driving factors of outsourcing.

As risk management is a very lively area for the research community in academics as well as corporate R&D departments we seek timely advice from practitioners on our thoughts and the proposed roadmap, also to gain an indicative validation on the likely success of our model.

Up to now we discussed the outline and some details of our approach with practitioners from internationally active banks and leading consulting companies. Talks have been conducted with five operational risk managers / controllers in large banks and three subject matter experts in international consulting companies, every interview partner being on director or senior management level.

Those first indicative talks have been encouraging. Key outcomes are:

- There is a strong practical need for that kind of assessment, as currently employed methodologies do not fully reflect the operational risk in outsourcing.
- The usage of Bayesian Belief Networks has explicitly been favoured within all interviews, but none of the companies has yet developed a working model.
- Interest is huge to gain theoretically founded insights in the outsourcing decision from an operational risk point of view.

In addition to the positive feedback we also got valuable comments on pitfalls detected through research or practical experience of our interview partners, which we include in our method.

All interview partners indicated the willingness for further talks as we develop our method further. These talks will be conducted on a regular basis to ensure a rigor yet relevant research and development approach.

5. Conclusion and further research

Within this paper we introduced a framework to classify and decompose operational risk in outsourcing in a way that generates quantifiable output (risk indicators) for the next phase of the risk management process, the measurement phase. The risk indicators can be transformed into a Bayesian Belief Network, which allows for scenario analyses.

This framework adds to the understanding of operational risk as its application enhances transparency through the transformation of often "fuzzy" described risks to precisely expressed risks that link directly to quantifiable parameters. This advantage is gained by supporting experts to specifically locate the source of risk and the potentially affected impact areas, which is the basis to name the quantifiable parameter, the risk indicator.

This paper represents part of a large research project on the management of operational risk in outsourcing. Next steps include an in depth research on the deployment of Bayesian Belief Networks for measurement purposes and on possible limitations to modelling operational risks. We currently use the software tool Hugin (www.hugin.com) to model a prototype network and the associated risk scorecard. An empirical validation of the outsourcing risks as identified in literature is planned for the near future via sending questionnaires to major banks in Germany. Finally we plan to conduct the empirical validation of the model with in depth case studies on two or more banks that either already outsourced part of their business or currently undergo the outsourcing decision process. The case studies should provide insights if

the model is able to handle the change in the risk structure before and after outsourcing and to cope with the desired scenario analyses.

Acknowledgement

The authors gratefully acknowledge the support of the *E-Finance Lab* at Frankfurt University.

6. References

Adeleye, B. C.; Annasingh, F. and Nunes, M. B.; Risk management practices in IS outsouring: an investigation into commercial banks in Nigeria, International Journal of Information Management, (24:2), 2004, pp. 167-180.

Alexander, M. and Young, D.; Strategic Outsourcing, Long Range Planning, (29:1), 1996, pp. 116-119.

Ang, S. and Toh, S.-K.; Failure in Software Outsouring: A Case Analysis in: Willcocks, L. P. and Lacity, M. C. (Eds.); Strategic Sourcing of Information Systems, John Wiley & Sons Ltd, Chichester, 1998, pp. 351-368.

Aubert, B. A.; Dussault, S.; Patry, M. and Rivard, S.; Managing the Risk of IT Outsourcing, 32nd Hawaii International Conference on System Sciences, 1999.

Aubert, B. A.; Patry, M. and Rivard, S.; Managing IT Outsourcing Risk: Lessons Learned in: Hirschheim, R., Heinzl, A. and Dibbern, J. (Eds.); Information Systems Outsourcing - Enduring Themes, Emergent Patterns and Future Directions, Springer, Berlin, 2002, pp. 155-176.

Bahli, B. and Rivard, S.; A Validation of Measures associated with the Risk Factors in Information Technology Outsourcing, 36th Hawaii International Conference on System Sciences, 2003.

Barthelemy, J.; The Hidden Costs of IT Outsourcing, MIT Sloan Management Review, (42:3), 2001, pp. 60-69.

Barthelemy, J. and Geyer, D.; IT Outsourcing: Evidence from France and Germany, European Management Journal, (19:2), 2001, pp. 195-202.

Basel Committee on Banking Supervision; The New Basel Capital Accord, (3rd) Consultative Document, 2003.

Brink, G. J. v. d.; Quantifizierung operationeller Risiken - Ein Weg zur Einbettung in den Managementzyklus, RiskNEWS, (Januar/Februar), 2003, pp. 26-36.

Caldwell, B. M.; IT Outsourcing Contracts: Crunching the Numbers, Gartner Dataquest, Research Brief, 2003.

Cross, J.; Earl, M. J. and Sampler, J. L.; Transformation of the IT Function at British Petroleum, MIS Quarterly, (21:4), 1997, pp. 401-423.

Davenport, T. H. and Short, J. E.; The New Industrial Engineering: Information Technology and Business Process Redesign, Sloan Management Review, (31:4), 1990, pp. 11-27.

Deutsche Bundesbank; Circular 11/2001 - Outsourcing of operational areas to another enterprise pursuant to section 25a (2) of the Banking Act, Frankfurt am Main, 2001.

Dibbern, J.; Goles, T.; Hirschheim, R. and Jayatilaka, B.; Information Systems Outsourcing: A Survey and Analysis of the Literature, The DATA BASE for Advances in Information Systems, (Forthcoming in 2004), 2004.

Earl, M. J.; Outsourcing Information Services, Public Money and Management, (Autumn), 1991, pp. 17-21.

Earl, M. J.; The Risks of Outsourcing IT, Sloan Management Review, (37:3), 1996, pp. 26-32.

Ebnöther, S.; Vanini, P.; McNeil, A. and Antolinez, P.; Operational Risk: A Practitioner´s View, Operational Risk, (11), 2002, pp. 1-15.

Federal Reserve Bank of New York; Summary of "Lessons Learned" and Implications for Business Continuity, Discussion note, available online at www.newyorkfed.org, 2002.

Gilley, K. M. and Rasheed, A.; Making More by Doing Less: An Analysis of Outsourcing and its Effects on Firm Performance, Journal of Management, (26:4), 2000, pp. 763-790.
Goodhart, C.; Operational Risk, London School of Economics - Special Paper No 131, 2001.
Halvey, J. K. and Melby, B. M.; Business Process Outsourcing - Process, Strategies and Contracts, John Wiley & Sons, New York, 2000.
Herring, R. J.; The Basel 2 Approach to Bank Operational Risk: Regulation on the Wrong Track, The Journal of Risk Finance, (Fall), 2002, pp. 42 - 45.
Hirschheim, R. and Dibbern, J.; Information Systems Outsourcing in the new Economy - An Introduction in: Hirschheim, R., Heinzl, A. and Dibbern, J. (Eds.); Information Systems Outsourcing - Enduring Themes, Emergent Patterns and Future Directions, Springer, Berlin, 2002, pp. 3-23.
Jorion, P. and Khoury, S. J.; Financial Risk Management, Blackwell Publishers, Cambridge, 1996.
Jurison, J.; A Risk-Return Model for Information Technology Outsourcing Decisions in: Willcocks, L. P. and Lacity, M. C. (Eds.); Strategic Sourcing of Information Systems, John Wiley & Sons Ltd,, Chichester, 1998, pp. 187-204.
Kakabadse, A. and Kakabadse, N.; Trends in Outsourcing: Contrasting USA and Europe, European Management Journal, (20:2), 2002, pp. 189-198.
Kern, T.; Willcocks, L. P. and Lacity, M. C.; Application Service Provision: Risk Assessment and Mitigation, MIS Quarterly Executive, (1:2), 2002, pp. 113-126.
Khalfan, A. M.; Information security considerations in IS/IT outsourcing projects: a descriptive case study of two sectors, International Journal of Information Management, (24:1), 2004, pp. 29-42.
Knight, F. H.; Risk, Uncertainty and Profit, Chicago, 1971.
Lacity, M. C.; Lessons in Global Information Technology, Computer, (August), 2002, pp. 26-33.
Lukacs, M.; Friend, M. and Snowdon, J.; European Business Process Outsourcing Forecast and Analysis 2001-2006, IDC, 2002.
McConnell, P. and Blacker, K.; An Approach to Modelling Operational Risk in Banks, Henley Working Paper No 9926, 1999.
McLellan, K.; Marcolin, B. L. and Beamish, P. W.; Financial and strategic motivations behind IS outsourcing, Journal of Information Technology, (10:4), 1995, pp. 299-321.
Netter, J. M. and Poulsen, A. B.; Operational Risk in Financial Service Providers and the Proposed Basel Capital Accord: An Overview in: Hirschey, M., John, K., Makhija, A., Hirschey, M., Kose, J. and Makhija, A. K. (Eds.); Corporate Governance and Finance (Advances in Financial Economics, Volume 8), 2003, pp. 147-171.
Pfleeger, S. L.; Risky business: what we have yet to learn about risk management, The Journal of Systems and Software, (53), 2000, pp. 265-273.
Quelin, B. and Duhamel, F.; Bringing Together Strategic Outsourcing and Corporate Strategy: Outsouring Motives and Risks, European Management Journal, (21:5), 2003, pp. 647-661.
Quinn, J. B. and Hilmer, F. G.; Strategic Outsourcing, Sloan Management Review, (35:4), 1994, pp. 43-55.
Renn, O.; Perception of Risk, The Geneva Papers on Risk and Insurance, (29:1), 2004, pp. 102-114.
Stambaugh, F.; Risk and Value at Risk, European Management Journal, (14), 1996, pp. 612-621.

Susaria, A.; Barua, A. and Whinston, A. B.; Understanding the Service Component of Application Service Provision: An Emperical Analysis of Satisfaction with ASP Services, MIS Quarterly, (27:1), 2003, pp. 91-123.

Tatikonda, M. V. and Montoya-Weiss, M. M.; Integrating Operations and Marketing Perspectives of Product Innovations: The Influence of Organizational Process Factors and Capabilities on Development Performance, Management Science, (47:1), 2001, pp. 151-172.

Willcocks, L. P.; Lacity, M. C. and Kern, T.; Risk Mitigation in IT outsourcing strategy revisited: longitudinal case research at LISA, Journal of Strategic Information Systems, (8:3), 1999, pp. 285-314.

7. Appendix

Detailed list of risks of outsourcing as identified in current IS literature (referred in section 3.1).

[Adeleye et al. 2004]
- Not achieving the planned benefits
- Not meeting agreed deadlines
- Using more resources than initially foreseen
- Change in functional and procedural requirements
- Budget overrun
- Deficient change over of systems, problems with the operation and maintenance of these systems

[Alexander and Young 1996]
- Hidden costs
- Impact on morale of staff
- Difficulties at the interfaces
- Poor service
- Supplier failing to deliver
- Costly switch to alternative supplier

[Aubert et al. 1999] (refined in [Aubert et al. 2002])
- Unexpected management and transition costs
- Switching costs (including lock-in, repatriation and transfer to another supplier)
- Costly contractual amendments
- Disputes and litigation
- Service debasement
- Cost escalation
- Loss of organizational competencies
- Hidden service costs

[Bahli and Rivard 2003]
- Asset Specifity
- Small number of suppliers
- Uncertainty
- Relatedness
- Measurement Problems
- Client / supplier expertise with the IT operation
- Client / supplier expertise with outsourcing

[Barthelemy and Geyer 2001]
- Union opposition
- Personnel opposition
- Personnel morale
- Cost (in depth discussed in [Barthelemy 2001])
- Quality
- Transition time
- Data leakage
- Know-how leakage
- Contract
- Dependency

[Earl 1996]
- Possibility of weak management
- Inexperienced staff
- Business uncertainty
- Outdated technology skills
- Endemic uncertainty
- Hidden costs
- Lack of organizational learning
- Loss of innovative capacity
- Danger of an Eternal Triangle
- Technological invisibility
- Fuzzy focus

[Jurison 1998]
- Irreversibility of the outsourcing decision
- Breach of contract by the vendor
- Loss of autonomy and control over IT decisions
- Vendor's inability to deliver
- Loss of control over vendor
- Uncontrollable contract growth
- Loss of critical skills
- Biased portrayal by vendors
- Vendor lock-in
- Loss over control of data
- Loss of employee morale and productivity
- Lack of trust
- Hidden costs

[Khalfan 2004]
- Security issues
- Ability to operate or manage new systems
- Loss of key IT employees
- Hidden costs (unspecified in the contract)
- Inadequate planning and management
- Loss of flexibility/control
- Lack of prior outsourcing experience

[Lacity 2002]
- Cost overruns
- Declining service levels
- Lack of innovation

[Quelin and Duhamel 2003]
- Dependence on the supplier
- Hidden costs
- Loss of know-how
- Service provider's lack of necessary capabilities
- Social risk

[Quinn and Hilmer 1994]
- Loss of critical skills or developing the wrong skills
- Loss of cross-functional skills
- Loss of control over supplier

[Willcocks et al. 1999]
- Treating IT as an undifferentiated commodity to be outsourced
- Incomplete contracting
- Lack of active management of the supplier on contract and relationship dimensions
- Failure to build and retain requisite in-house capabilities and skills
- Power asymmetries developing in favour of the vendor
- Difficulties in constructing and adapting deals in the face of rapid business/technical change
- Lack of maturity and experience of contracting for and managing "total" outsourcing arrangements
- Outsourcing for short term financial restructuring or cash injection rather than to leverage IT assets for business advantage
- Unrealistic expectations with multiple objectives for outsourcing
- Poor sourcing and contracting for development and new technologies