IT Security Risk Management

Tobias Ackermann

IT Security Risk Management

Perceived IT Security Risks in the Context of Cloud Computing

Springer Gabler

Tobias Ackermann
Fachgebiet Wirtschaftsinformatik
TU Darmstadt
Darmstadt, Germany

Dissertation Technische Universität Darmstadt, 2012

D 17

ISBN 978-3-658-01114-7 ISBN 978-3-658-01115-4 (eBook)
DOI 10.1007/978-3-658-01115-4

The Deutsche Nationalbibliothek lists this publication in the Deutsche Nationalbibliografie; detailed bibliographic data are available in the Internet at http://dnb.d-nb.de.

Library of Congress Control Number: 2012955651

Springer Gabler
© Springer Fachmedien Wiesbaden 2013
This work is subject to copyright. All rights are reserved by the Publisher, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, reuse of illustrations, recitation, broadcasting, reproduction on microfilms or in any other physical way, and transmission or information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed. Exempted from this legal reservation are brief excerpts in connection with reviews or scholarly analysis or material supplied specifically for the purpose of being entered and executed on a computer system, for exclusive use by the purchaser of the work. Duplication of this publication or parts thereof is permitted only under the provisions of the Copyright Law of the Publisher's location, in its current version, and permission for use must always be obtained from Springer. Permissions for use may be obtained through RightsLink at the Copyright Clearance Center. Violations are liable to prosecution under the respective Copyright Law. The use of general descriptive names, registered names, trademarks, service marks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and regulations and therefore free for general use. While the advice and information in this book are believed to be true and accurate at the date of publication, neither the authors nor the editors nor the publisher can accept any legal responsibility for any errors or omissions that may be made. The publisher makes no warranty, express or implied, with respect to the material contained herein.

Printed on acid-free paper

Springer Gabler is a brand of Springer DE.
Springer DE is part of Springer Science+Business Media.
www.springer-gabler.de

Foreword

Since many years, IT outsourcing is a widespread and actively used opportunity to transfer IT functions to third parties and thereby reduce costs. In recent years, the current trend in the form of Cloud Computing, i. e., the sourcing of applications, computing power and storage space over the Internet, is increasingly discussed by scientists and practitioners. However, the promised benefits of Cloud Computing are accompanied by a growing number of IT security incidents that are, on the one hand, a problem for the users, as they may not be able to access and use the service or because the confidentiality of their customer data may be compromised. On the other hand, such security incidents are also a problem for the service providers as they may jeopardize their reputation and may lose customers.

Therefore, the research objective of this thesis is to analyze the perception and effect of IT security risks of Cloud Computing in detail. First, the relevant IT security risks of Cloud Computing are identified and systematized in a structured process, in order to later use them as a part of an empirical survey. A quantitative empirical survey is used to examine how potential users perceive IT security risks as well as how these risk estimations affect the adoption of Cloud Computing. At the end, using a mathematical model specifically designed for the characteristics of Cloud Computing scenarios, it is investigated how parameters of a scenario affect the distribution of potential losses.

This thesis's first part addresses the analysis of the various IT security risks of Cloud Computing and their perception. In order to identify the individual components of the concept "IT security", Mr. Ackermann first presents a structured literature review. The iterative refinement of search results and the following process of extracting all relevant individual risks and clustering them to risk dimensions are thoroughly described. Mr. Ackermann uses the Q-sort method to systematically evaluate the resulting taxonomy. In order to further refine and evaluate the individual risk descriptions, he conducts qualitative interviews with 24 IT security

experts. Thereby, the exhaustiveness of the list of risks is ensured and it is possible to discover five previously not published individual risks. Subsequently, the formal specification of the latent construct "Perceived IT Security Risk" is described and the relationships and effects between the individual constituting dimensions and their risks is discussed. Finally, after describing the setup of the quantitative empirical survey, the validation of the developed scale is presented. In addition to traditional tests of the goodness of fit and the validity and reliability of indicators and constructs, the scale is also tested using more advanced tests, such as known-groups comparison or tests for nomological and multidimensional validity.

Mr. Ackermann makes several significant contributions to information systems science: In addition to the developed scale, the analysis of the effects of the perceived IT security risks on the potential users' adoption decisions contributes to information systems literature. Based on the theory of reasoned action and previous studies, he derives hypotheses about the decision processes of IT executives. The hypotheses are analyzed in the form of structured equation models and their validity is confirmed using the responses of the quantitative study. The results show that the perceived IT security risk has a double detrimental effect on Cloud Computing adoption decisions.

In this thesis's second part, Mr. Ackermann develops a mathematical risk quantification framework which can be used to support the IT risk management process for Cloud Computing scenarios. He describes methods with which it is possible to identify the individual risk or component that introduces the biggest share of the overall aggregated risk distribution. The results of the sensitivity analysis indicate that scenarios are more sensitive to changes in the amount of the potential losses, while changes to the occurrence probabilities or the number of risks have a smaller effect on the resulting distribution. Moreover, the framework is applied to an existing e-commerce system where two alternative security levels are compared to each other in order to find the most economically reasonable countermeasures. Additionally, the cost drivers of the scenario are identified with the help of the presented methods.

The entire scale development process as well as the mathematical model's analysis show a great degree of methodological rigor and provide many interesting results. This thesis will be valuable to readers in both, academia and practice, as it suggests concrete recommended actions for users and providers of Cloud Computing services that can be applied during IT risk management. Therefore, I wish this thesis a widespread distribution.

Darmstadt, September 2012 *Prof. Dr. Peter Buxmann*

Preface

This thesis was written during my work as a research assistant at the chair of Information Systems | Software Business & Information Management at the Technische Universität Darmstadt.

I am especially grateful for my supervisor Prof. Dr. Peter Buxmann, who greatly supported me and gave me many helpful suggestions. Likewise, I would like to thank my second referee Prof. Dr. Alexander Benlian for his valuable advises.

Furthermore, I thank the CASED graduate school for the granting of a PhD scholarship as well as numerous CASED postdocs and PhD students with whom I conducted the qualitative interviews.

My special thanks go to my friends and colleagues Alexander, André, André, André, Andreas, Anne, Anton, Björn, Christoph, Cornelia, Daniel, Eva, Florian, Golriz, Janina, Jasmin, Jin, Kerstin, Leonardo, Mark, Markus, Markus, Michael, Oliver, Omid, Patrick, Ruth, Sebastian, Sebastian, Sheikh, Sonja, Stefan, Sunil, Thomas, Thomas, Thorsten, Tobias und Tolga, whom I thank wholeheartedly for their support.

Darmstadt, September 2012 *Tobias Ackermann*

Contents

List of Figures

List of Tables

Acronyms

ACM	Association for Computing Machinery
AES	Advanced Encryption Standard
AISeL	AIS Electronic Library
API	Application Programming Interface
ASP	Application Service Provision
AVE	Average Variance Extracted
BPEL	Business Process Execution Language
BPO	Business Process Outsourcing
BSP	Business Source Premier
CEO	Chief Executive Officer
CFI	Comparative Fit Index
CIO	Chief Information Officer
CLo	Customer Location
CMB	Common Method Bias
CPU	Central Processing Unit
CR	Construct Reliability
CRa	Customer Rating
CSA	Covariance Structure Analysis
CSRF	Cross Site Request Forgery
CSS	Cascading Style Sheets
DDoS	Distributed Denial of Service
df	degrees of freedom
DoS	Denial of Service
DPP	Dynamic Posted Pricing
DT	Data Transfer
ECIS	European Conference on Information Systems
EDI	Electronic Data Interchange

ENISA	European Network and Information Security Agency
ERP	Enterprise Resource Planning
GFI	Goodness of Fit Index
HTML	Hypertext Markup Language
HTTPS	Secure Hypertext Transfer Protocol
IaaS	Infrastructure as a Service
ICIS	International Conference on Information Systems
IDS	Intrusion Detection System
IEEE	Institute of Electrical and Electronics Engineers
IIA	Intention to Increase Adoption
IP	Internet Protocol
IS	Information Systems
IT	Information Technology
ITO	Information Technology Outsourcing
JAIS	Journal of the Association for Information Systems
JSON	JavaScript Object Notation
KPI	Key Performance Indicator
LISREL	Linear Structural Relations
MECE	Mutually Exclusive and Collectively Exhaustive
MIMIC	Multiple Indicators, Multiple Causes
MIS	Management Information Systems
NFI	Normed Fit Index
NIST	National Institute of Standards and Technology
NNFI	Non-Normed Fit Index
OSP	Online Shop Pricing
PaaS	Platform as a Service
PDFL	Probability Density Function of the Potential Losses
PHP	PHP: Hypertext Preprocessor
PITSR	Perceived IT Security Risk
PLS	Partial Least Squares
PNU	Perceived Negative Utility
PPU	Perceived Positive Utility
RMSEA	Root Mean Square Error of Approximation
ROI	Return on Investment
ROSI	Return on Security Investment
SaaS	Software as a Service
SEM	Structural Equation Model
SHA	Secure Hash Algorithm
SLA	Service Level Agreement
SME	Small and Medium Enterprises
SQL	Structured Query Language

SRMR	Standardized Root Mean Square Residual
SSL	Secure Sockets Layer
TAM	Technology Acceptance Model
TLI	Tucker Lewis Index
TRA	Theory of Reasoned Action
UTAUT	Unified Theory of Acceptance and Use of Technology
VaR	Value-at-Risk
VIF	Variance Inflation Factor
VM	Virtual Machine
VPN	Virtual Private Network

Abstract

Despite increasing interest in Information Technology (IT) outsourcing and the various benefits it promises, Cloud Computing as the currently most prevalent IT outsourcing paradigm still presents various crucial IT security risks for companies. Although the Information Systems (IS) field increasingly recognizes the importance of IT security risks in Cloud Computing adoption decision-making processes, little attention has been paid so far to fully capture the complex nature of IT security risk and better understand its inhibitory role. Furthermore, traditional IT risk management methods cannot be directly applied in Cloud Computing contexts, when data are sent to, stored, and processed by external providers, as these methods were developed for traditional in-house IT architectures.

Against this backdrop, the first part of this thesis proposes a comprehensive conceptualization of perceived IT security risk in the Cloud Computing context that is based on six distinct risk dimensions grounded on a structured literature review, Q-sorting, and expert interviews. Second, a multiple-indicators and multiple-causes analysis of data collected from 356 organizations is found to support the proposed conceptualization as a second-order aggregate construct. Third, the effects of perceived IT security risks on negative and positive attitudinal evaluations in IT executives' Cloud Computing adoption decisions are examined. The empirical results demonstrate that high IT security risk perceptions not only fuel negative evaluations of Cloud Computing. Rather, such perceptions may turn out to be a double curse because they simultaneously devalue positive assessments of Cloud Computing exacerbating reluctance to adopt Cloud Computing services. The second part of this thesis presents a mathematical risk quantification framework that can be used to support the IT risk management process of Cloud Computing users. Based on simulation results, the influence of individual IT security risk parameters on the overall aggregated risk distribution is analyzed. Furthermore, methods

for the identification of cost drivers are described and the effects of introducing inaccuracies are examined.

The combination of results, obtained through the conceptualization and assessment of perceived IT security risk as well as the mathematical IT security model, contributes to IT security and IT outsourcing research, supports the IT risk management processes of (potential) adopters during risk identification, quantification, and treatment, and enables Cloud Computing providers to develop targeted strategies to mitigate risks perceived as crucial.

Zusammenfassung

Trotz des steigenden Interesses an Information Technology (IT) Outsourcing und den zahlreichen Vorteilen, die es verspricht, ist die Nutzung von Cloud Computing, der aktuell am stärksten verbreiteten Form von IT Outsourcing, immer noch mit verschiedensten IT Sicherheitsrisiken verbunden. Obwohl die Information Systems (IS) Forschung zunehmend die Relevanz von IT Sicherheitsrisiken für die Verbreitung von Cloud Computing anerkennt, wurde einer umfassenden Konzeptualisierung von IT Sicherheitsrisiken bisher wenig Aufmerksamkeit geschenkt. Zusätzlich lassen sich traditionelle Methoden des IT Risikomanagements nicht direkt im Kontext von Cloud Computing einsetzen wenn Daten zu externen Providern gesendet und dort verarbeitet und gespeichert werden, da diese Methoden nur für unternehmensinterne Architekturen entwickelt wurden.

Vor diesem Hintergrund stellt der erste Teil dieser Dissertation eine umfassende Konzeptualisierung des wahrgenommenen IT Sicherheitsrisikos im Kontext von Cloud Computing vor, die aus sechs Risikodimensionen besteht und auf einer strukturierten Literaturrecherche, Q-Sorting und Expertengesprächen basiert. Eine „Multiple-Indicators Multiple-Causes Analyse“ der von 356 Unternehmen in einer großzahligen Studie erhobenen Daten unterstützt die Konzeptualisierung als zusammengesetztes Second-Order Konstrukt. Zusätzlich werden die Auswirkungen des wahrgenommenen IT Sicherheitsrisikos auf die negativen und positiven Einstellungen gegenüber Cloud Computing im Rahmen von Entscheidungsprozessen von IT Leitern untersucht. Die empirischen Daten zeigen, dass hohe IT Sicherheitsrisiken nicht nur die negativen Bewertungen von Cloud Computing verstärken, sondern gleichzeitig auch die Wertschätzung der positiven Eigenschaften verringern. Der zweite Teil der Dissertation beschreibt ein mathematisches Modell zur Risikobewertung, das den IT Risikomanagementprozess von Cloud Computing Nutzern unterstützen kann. Basierend auf Simulationen wird der Einfluss einzelner Parameter von IT Sicherheitsrisiken auf die gesamte, aggregierte Risikoverteilung

untersucht. Zusätzlich werden Methoden zur Identifikation von Kostentreibern vorgestellt und der Effekt von Ungenauigkeit der Parameter analysiert.

Die Kombination der Ergebnisse, die durch die Konzeptualisierung und Bewertung des wahrgenommenen IT Sicherheitsrisikos sowie durch das mathematische Modell erzielt wurden, trägt zur IT Sicherheits- und IT Outsourcing-Literatur bei, unterstützt das IT Risikomanagement von (potentiellen) Nutzern und ermöglicht es Cloud Computing Anbietern, gezielte Maßnahmen zu entwickeln, um die als kritisch wahrgenommenen Risiken zu vermindern.

Chapter 1
Introduction

1.1 Problem Description and Motivation

Over the last couple of decades, the majority of companies have outsourced at least parts of their information systems to external suppliers, and a broad stream of research has been dedicated to the phenomenon of Information Technology Outsourcing (ITO). This development has been reinforced further by the currently much-discussed approach of "Cloud Computing" (Mell and Grance, 2011). Cloud Computing applications can be differentiated as Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS) applications, depending on the type of capability provided (Vaquero et al., 2009).

Cloud Computing promises to deliver all of the functionality of existing Information Technology (IT) services at dramatically-reduced upfront costs compared to other new technologies (Marston et al., 2011, p. 176). These promises led to high expectations for the Cloud Computing market. According to market forecasts, the public Cloud Computing service market is large and growing, although exact numbers vary widely: Gartner expects the worldwide Cloud Computing services revenue (including public and private services) to be a $150 billion business by 2014 (Pring et al., 2010), while AMI partners expect that Small and Medium Enterprises (SME) are going to spend more than $95 billion on Cloud Computing by 2014. Research done by Merrill Lynch even predicts that the Cloud Computing market will be worth $160 billion by the year 2013.

Besides various technical and economic advantages of ITO in general and the "Cloud" in particular (Marston et al., 2011), ITO still presents various crucial IT security risks for companies.

Although strong efforts have been made to mitigate these risks in the past (Pring, 2010), various recent security incidents related to Cloud Computing em-

T. Ackermann, *IT Security Risk Management,* DOI 10.1007/978-3-658-01115-4_1,
© Springer Fachmedien Wiesbaden 2013

phasize the risks still faced by ITO adopters: The Amazon EC2 Cloud Computing services crashed in April 2011, resulting in painful data loss for hundreds of clients; in August 2011, a lightning strike was the cause behind the downtime of Microsoft's Cloud Computing service "Business Productivity Online Suite", preventing the affected client companies from accessing e-mails, calendars, contacts, and the document management system for about 48 hours.

These accidents illustrate the tremendous effects Cloud Computing-related security incidents can have on the businesses of the customers as well as the importance of proper IT risk management.

In addition to directly-affected users, broad coverage of these incidents in the mainstream-media has reached a large number of current and potential customers, and has had a devastating effect on the reputation of respective providers – causing an undefined amount of lost sales. This media coverage is especially relevant in view of the fact that, in many cases, it is not the *actual* IT security risk that might be crucial in deciding to outsource IT; often, it is the risk *perceived* by the CIO/CEO that triggers such decisions. This fact has already been recognized in other disciplines; for example, Gigerenzer (2004) showed that after September 11, a great deal of travelers avoided air travel (which is typically low-risk), preferring to travel by car or bus, which resulted in approximately 350 additional lives lost due to fatal accidents. This misjudgment of so-called "dread risks" (i. e., high-impact, low-probability incidents such as a terrorist attack or a lightning strike at a datacenter) is a phenomenon that has already been acknowledged in broader risk literature (Slovic, 1987). Better understanding the perceived risk and knowledge of such "risk controversies" in the outsourcing and, more specifically, Cloud Computing contexts would allow current and potential users to better assess risks, as well as allow providers of Cloud Computing solutions to better address the users' (sometimes unjustified) fears.

Accordingly, researchers in our discipline have shown increased interest in incorporating security risks in outsourcing considerations (e. g., Hahn et al., 2009; Swartz, 2004); however, although previous research studies repeatedly found that IT security risks are one of, if not the main risk factor considered in important outsourcing and adoption decisions (e. g., Benlian and Hess, 2011), there has been little discussion about the complex nature of (perceived) IT security risks, the conceptualization of this construct, and the identification of the constituting dimensions of this concept. Consequently, previous studies have been forced to incorporate simple and one-dimensional measures for perceived IT security risks.

Contrary to the high expectations of the Cloud Computing market by Gartner, AMI, and Merrill Lynch, some companies and market researchers are particularly skeptical about Cloud Computing's viability and applicability in strong markets of enterprise application software, such as Enterprise Resource Planning (ERP).

Major barriers to Cloud Computing's adoption are said to be reliability issues (i. e., stable access to services), information security and privacy concerns (i. e., security breaches and improper protection of sensitive firm data), and process dependence (i. e., performance measurement and service quality), as Benlian et al. (2009) found for SaaS applications. Security risks and cost advantages are the most prominent factors forming IT executives' overall opportunity-risk appraisal. Therefore, security risks are an important determinant of firms' attitudes towards Cloud Computing (Benlian and Hess, 2011).

Conversely, existing findings on risk assessments are rather abstract in that there are no in-depth empirical analyses to ascertain which IT security risk factors associated with Cloud Computing are most influential in forming firms' adoption decisions.

In order to reduce the risks involved in the use of Cloud Computing, (potential) users of this technology need to apply specific IT risk management procedures informed by some of the characteristics of Cloud Computing. Unfortunately, most traditional methods (see Prokein (2008) for a collection) cannot be directly applied in Cloud Computing contexts, when data are sent to, stored, and processed by external providers, as these methods were developed for traditional in-house IT architectures. In particular, information systems based on Cloud Computing deal with a large set of potential risks that are associated with high potential losses, e. g., confidentiality- and availability-related risks.

Farahmand et al. (2008) list the quantification of IT security incidents as one of the key questions for further research on risk management. Considering the dynamic nature of technologies as well as changing network and IT environments, it becomes more and more clear how important it is to provide efficient risk assessment and management methods.

1.2 Objectives and Benefit

This thesis's main objective is to analyze IT security in the context of Cloud Computing and to improve support for IT executives in implementing proper IT risk management. In particular, this dissertation will examine four main research questions:

1. What are the IT security risks present in the context of Cloud Computing and how can they be systematized?
2. How do IT executives perceive the IT security risks of Cloud Computing?
3. Which IT security risks influence IT executives' adoption decisions related to Cloud Computing?
4. Which risk parameters influence IT security in the context of Cloud Computing scenarios?

Because previous IT security risk studies relied on simple, unidimensional and/or inconsistent conceptualizations (e. g., Chellappa and Pavlou, 2002; Flavián and Guinalíu, 2006; Casalo et al., 2007; Kim et al., 2008; Pavlou et al., 2007), one of the main objectives of this thesis is to systematically develop a comprehensive and unambiguous meaning (i. e., conceptualization) and measurement (i. e., operationalization) of Perceived IT Security Risk (PITSR), particularly in the context of Cloud Computing.

By addressing the first research question, this thesis makes several theoretical contributions: First, we propose a conceptual framework for perceived IT security risks and provide an in-depth conceptualization for Cloud Computing grounded on an extensive literature review and expert interviews. This enhanced framework and conceptualization of perceived IT security risk can be used to enhance various existing theories, e. g., through incorporation of perceived IT security risks in theories that explain outsourcing and adoption decisions such as the Technology Acceptance Model (TAM) (Davis, 1989), the Theory of Reasoned Action (TRA) (Ajzen, 1985), or the Unified Theory of Acceptance and Use of Technology (UTAUT) (Venkatesh et al., 2003). Second, we develop a measurement scale, which provides a comprehensive operationalization of IT security risks in the context of Cloud Computing that captures its complex, multi-dimensional nature and therefore establishes a basis for further empirical research on the effects of perceived IT security risks on outsourcing decisions.

Existing risk literature shows that risk is usually considered to be composed of sub-scales and multiple risk dimensions that are perceived separately (i. e., each with an individual intensity) from each other (e. g., Peter and Tarpey, 1975; Havlena and DeSarbo, 1990; Mitchell and Greatorex, 1993; Featherman et al.,

2006; Benlian and Hess, 2011). So far, IT security risks related to Cloud Computing have not been analyzed in-depth; therefore, this thesis provides the first detailed assessments of the perceptions of IT executives in this context.

The measurement scale, which is validated using assessments obtained by a survey among 6,000 German companies, can be used to study how collected IT security risks aggregate to the composite latent PITSR construct. Furthermore, it is possible to extract the dominant risks that form large portions of the overall perceived risk. Likewise, risks that are perceived to be uncritical or do not play an important role during the aggregation are identified.

Previous research studies repeatedly found that IT security risks are one of, if not the major risk factor affecting Cloud Computing adoption decisions (e. g., Benlian and Hess, 2011). Nevertheless, present conceptualizations of this new category of risks lack the comprehensiveness that previous research has achieved regarding other classes of risks related to ITO (e. g., Earl, 1996; Bahli and Rivard, 2005; Lacity et al., 2009). Consequently, there has been little discussion about the effect of perceived IT security risks on IT executives' Cloud Computing adoption intentions.

Based on the conceptualization and the results of the survey, this thesis aims to contribute to a better understanding of the effect of IT security risks on Cloud Computing adoption decisions. By doing so, we shed light on the dual detrimental role of PITSR: those risks not only nurture the perceived negative utility but also abate the perceived positive utility of Cloud Computing at the same time.

The current Cloud Computing trend raises the demand for new IT risk management approaches that incorporate the special (i. e., graph-based) structure of such architectures: hard- and/or software, such as servers or services, (nodes) are interconnected by data transfers (edges), and are thereby orchestrated to complex information systems. In addition, and on a higher level of abstraction, it is possible to treat most information systems as scenarios that consist of hard- and software as well as data transfers. Since traditional models for security investment decisions (e. g., Gordon and Loeb, 2002; Soo Hoo, 2000; Wang et al., 2008) are not able to incorporate these aspects, new risk management methods for composed information systems have to be developed.

Based on a mathematical model, we analyze which security risk parameters influence the overall IT security of Cloud Computing scenarios. Using a simulation-based approach, we identify the individual effects of these parameters – such as occurrence probabilities, potential losses, number of risks, and number of components – and show how the overall risk changes when a parameter value is reduced or increased. Knowledge of individual effects allows decision makers to better prioritize their strategies for risk treatment. Additionally, it is possible to more ac-

curately anticipate how the overall risk is going to change when the scenario is altered.

In addition to these theoretical contributions, this thesis provides several practical benefits. Answering our four research questions will allow decision makers to adequately manage the IT security risks that can arise when Cloud Computing is used as a sourcing model. The combination of results obtained through the conceptualization and assessment of PITSR as well as the mathematical IT security model supports the processes during risk identification, quantification, and treatment.

The taxonomy of IT security risks can be used as a checklist in order to identify risks related to specific scenarios. The perceptions of other IT executives can be used as references when risks related to individual scenarios are assessed. Knowledge of risk parameters and their effects helps decision makers to better analyze the potential losses that can arise if Cloud Computing is used.

Additionally such a conceptualization and operationalization (including the assessments of these risks by IT experts) may allow (potential) users to quantify risks in individual Cloud Computing-related scenarios, and enable providers to develop strategies to better manage and mitigate those risks.

In this thesis, we contribute a model that supports Information Systems (IS) security-related investment decisions in service-based information systems. It allows for the assessment of cost-benefit trade-offs related to security measures esp. by solving the key problem of calculating the probability density function of potential losses (i. e., potential losses and their respective occurrence probabilities; see figure 4.15 for an example) for a given scenario. Recent publications acknowledge the fact that companies make investment choices based on individual risk preferences and not solely on mean values (i. e., they are not purely risk-neutral and take the variance of losses into account) (Wang et al., 2008, pp. 107f.). By building on our model and the calculated probability density function of potential losses, individual "attractiveness" metrics, such as the expected value, the Value-at-Risk (Jorion, 2006), or more complex utility functions, such as the μ-σ-rule using individual risk preferences, can be derived. Based on these metrics, decision makers can assess the attractiveness of alternative scenarios and choose the optimal security level, i. e., the most economically reasonable combination of security measures.

Additionally, using the model, it is possible to show how the aggregated risk is concentrated in individual scenario components, as a fraction of the overall risk. Thus, decision makers can analyze which components of the system (e. g., services and data transfers) induce the highest proportion of risk and whose removal or exchange leads to the largest reduction of potential losses during the IT risk treatment phase. This identification of cost drivers supports the understanding of how risks emerge and propagate in the system, and shows where countermeasures

can best be implemented. Therefore, this approach can be used in order to evaluate and prioritize security measures.

Furthermore, it is possible to perform the task of service selection, in which a decision maker can choose among candidates for some or all services. This can be done by calculating the attractiveness (e. g., cost for the service combination vs. Value-at-Risk) for each combination of candidates and selecting the combination with the highest assessment.

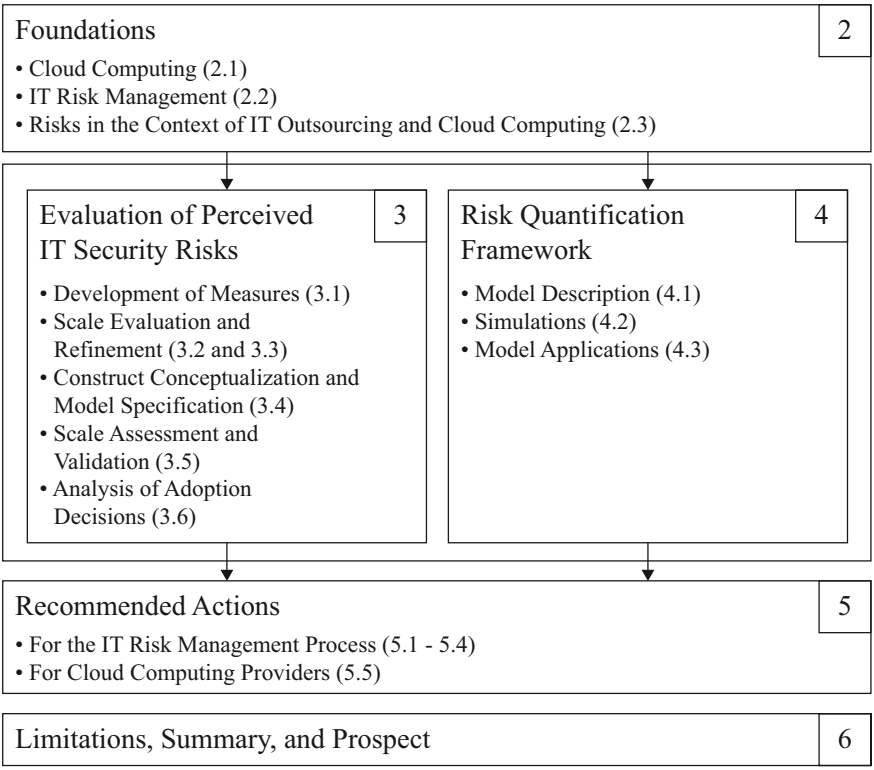


Figure 1.1 Structure of this Dissertation

1.3 Structure of this Dissertation

The remainder of this thesis is structured as shown in figure 1.1. Table 1.1 shows which sections are related to our four research questions presented in section 1.2. The foundations of relevant technologies and the theoretical background are introduced in chapter 2. The underlying paradigm of Cloud Computing, along with its core technological concepts and terminology, is described in section 2.1. Section 2.2 presents the IT risk management process as well as its four phases in more detail. Finally, work related to risks in the context of ITO and Cloud Computing is presented in section 2.3.

Based on these foundations, the main part of this thesis is divided into two major components: First, chapter 3 presents an in-depth evaluation of perceived IT

Table 1.1 Mapping of Questions to Research Methods and Chapters

	Scale Development				Survey		Modeling & Simulation		
	3.1: Literature Review	3.2: Q-Sort Method	3.3: Expert Interviews	3.4: Formal Model Specification	3.5: Scale Validation	3.6: Analysis of Adoption Decisions	4.1: Model Description	4.2: Simulations	4.3: Model Application
What are the IT security risks present in the context of Cloud Computing and how can they be systematized?	✓	✓	✓	✓	✓				
How do IT executives perceive the IT security risks of Cloud Computing?					✓				
Which IT security risks influence IT executives' adoption decisions related to Cloud Computing?						✓			
Which risk parameters influence IT security in the context of Cloud Computing scenarios?							✓	✓	✓

security risks in the context of ITO and Cloud Computing. Second, a mathematical risk quantification framework is described in chapter 4.

In the first part of chapter 3, sections 3.1 to 3.5, we present a rigorous scale development approach by which we develop, refine and evaluate a multi-dimensional conceptualization of perceived IT security risks and a corresponding measurement instrument.

The scale development and evaluation approach consists of five steps: (1) the development of measures, i. e., IT security risks, using a structured literature review (section 3.1), scale evaluation and refinement (2) using the Q-sort method (section 3.2) as well as (3) qualitative interviews among security researchers (section 3.3), and (4) conceptualization of the construct and specification of the measurement model (section 3.4). In the final step (5), the scale is validated using an empirical survey among IT executives in section 3.5. The systematically derived security risk taxonomy answers our first research question. By validating the scale

using data collected from 356 organizations through a large survey, we answer the second research question. The survey responses contain valuable assessments of the perceived IT security risks by IT executives, and they show which risks are perceived to be most serious.

In the second part of chapter 3, we analyze which specific risks are most influential in forming firms' adoption decisions in section 3.6. Therein, we analyze the impact of positive and negative attitudinal appraisals of Cloud Computing adoption on behavioral intentions based on the in-depth conceptualization of Perceived IT Security Risk (PITSR) and the developed measurement scale. Additionally, we also assess which specific risks are most influential in forming firms' adoption decisions which answers our third research question.

In chapter 4, we present a mathematical risk quantification framework that can be used to support the IT risk management process described in section 2.2. The model – including its parameters as well as related equations and algorithms – is introduced and described in section 4.1. The second section (section 4.2) describes simulations and methods regarding sensitivity analysis, identification of cost drivers, and the introduction of inaccuracy. These results will be used to identify which parameters of Cloud Computing scenarios influence the IT security and to what extent. This provides answers regarding our fourth research question. Finally, in section 4.3, we demonstrate the model's application in the context of an existing real-life e-commerce system by evaluating and comparing two alternative security investments for this business process.

Chapter 5 combines the results of chapters 3 and 4, and describes recommended actions for the individual phases of the IT risk management process for Cloud Computing users. Additionally, the chapter also provides recommended actions for Cloud Computing providers.

Finally, we conclude and discuss limitations as well as the theoretical, methodological and practical implications of our study's results in chapter 6.

Chapter 2
Foundations

2.1 Cloud Computing

Cloud Computing is based on the idea that resources, such as software applications, Central Processing Unit (CPU) capacity, and data storage, are no longer processed, kept, and stored at the users' side. Instead, they are centrally and dynamically provided by the provider over networks, e. g., the Internet (Buxmann et al., 2011b, p. 21). The National Institute of Standards and Technology (NIST) defines Cloud Computing as "a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e. g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction" (Mell and Grance, 2011, p. 2).

Thereby, Cloud Computing is based on the principle of virtualization and allocation of IT-based services to worldwide distributed computers. From an economic perspective, the providers have the advantage that they use available resources more effectively and realize supply-side economies of scale. Therefore, it is not surprising that particularly large providers such as Amazon, Google, and Microsoft tap into this market (Buxmann et al., 2011a, p. 11).

Next to the definition of Cloud Computing, NIST defines five essential characteristics in order to specify the paradigm (Mell and Grance, 2011, p. 2; Baun et al., 2011, pp. 3f.). The essential characteristics are:

On-demand self service. Users of a Cloud Computing service can request resources, such as computing and storage capacity, independently from the provider and according to their needs without having to rely on human interaction with the service provider. Since the provided resources are managed

T. Ackermann, *IT Security Risk Management,* DOI 10.1007/978-3-658-01115-4_2,
© Springer Fachmedien Wiesbaden 2013

through software, they can be scaled with minimal service provider interaction (Marston et al., 2011, p. 178).

Broad network access. Access to the resources and services is network-based and occurs in real-time using standard technologies and mechanisms such as the Internet and web interfaces. This lightweight accessibility makes Cloud Computing services more easy to use for potential customers (Weinhardt et al., 2009, p. 394).

Resource pooling. The vendor-supplied resources are consolidated into pools and allow parallel use by several users. The resources can be customized (e. g., in terms of amount, speed, and functionality) to match the actual needs of each user. A specific feature of Cloud Computing is that the user has no knowledge and no control over where the provided resources are exactly located. However, sometimes it is possible to specify the location on a higher level of abstraction, e. g., by country, region, or data processing center (Streitberger and Ruppel, 2009, p. 6).

Rapid elasticity. Resources can be provided quickly and in different, finely granulated quantities, thus, allowing the system to reconfigure and scale dynamically (Vaquero et al., 2009, p. 54). This creates the impression of infinite resources that are available at any time. Additionally, it is also possible to quickly decrease unused resources (i. e., release them) when they are no longer required (Mather et al., 2009, p. 8).

Measured service. Cloud Computing systems automatically control and optimize the use of their resources. The resource usage is monitored, controlled, and reported, which provides transparency for both the clients and the provider of the service (Weinhardt et al., 2009, p. 392).

Cloud Computing is often structured into three consecutive layers which represent different service delivery models: Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS). An extended Cloud Computing stack architecture that additionally contains information from crowds of people and supporting services in presented by Lenk et al. (2009).

Infrastructure as a Service. The providers on the IaaS layer supply infrastructure resources, such as storage, networking and processing capacity, and allow their customers to upload and run arbitrary, individual software. The providers thereby abstract the customers' view of the physical hardware. By using virtualization, it is possible to automatically "split, assign, and dynamically resize these resources" (Vaquero et al., 2009, p. 51). Hence, the customers usually do not know, where or in which servers exactly their data are processed. Examples for IaaS include Amazon's EC2 computing platform and the S3 storage service (Buyya et al., 2008, pp. 9f.).

Platform as a Service. On the PaaS layer, platform solutions, such as, e. g., development platforms, are provided based on the infrastructure of a Cloud Computing offering. The platforms provide development tools and Application Programming Interfaces (APIs) for interacting with the platform as well as a runtime environment. This facilitates the development and deployment of applications as the PaaS clients do not need to invest in the infrastructure nor manage its complexity (Marston et al., 2011, p. 178). Examples of PaaS include Microsoft's Azure Services Platform, Google App Engine, Salesforce's application development platform Force.com, Amazon's Relational Database Services, and Rackspace Cloud Sites.

Software as a Service. The usage of standard software solutions as a service over the Internet is referred to as SaaS (Buxmann et al., 2008, p. 500). Thereby, the provider offers its customers access to web-based applications, and takes care of managing the operation and maintenance of the application and the underlying hardware and software layers. While SaaS solutions generally offer many possibilities for pricing strategies, usage-independent fees, e. g., based on the number of users, are common (Lehmann and Buxmann, 2009, p. 523). Contrary to traditional, isolated software installations, SaaS typically uses the one-to-many delivery approach which is also called "multitenancy". This principle refers to architectures, where a single software instance, running on a server, serves multiple tenants (i. e., the client organizations) at the same time (Mather et al., 2009, p. 18). This model of service delivery eliminates the need to install the application on the client computer as the software is accessed using a standard web browser and usually runs over existing public networks, i. e., Internet access infrastructure (Marston et al., 2011, p. 178). Examples are Google Apps, SAP BusinessByDesign, Netsuite, or salesforce.com.

2.2 IT Risk Management

After a short introduction of risk-related definitions in section 2.2.1, the common phases of the IT risk management process are discussed in more detail in section 2.2.3.

2.2.1 Risk-related Definitions

In IS and economics research, an agreed definition of *risk* has not been arrived at and there are many different concepts of risk. The word "risk" is derived from the Italian word "riscare" which means "to dare something" and, therefore, contains negative as well as positive components (Wolke, 2008, p. 1).

In contrast, most of the currently-used definitions are primarily focused on negative deviation from an expected target state (Prokein, 2008, p. 7). These more recent definitions refer to possible damages or potential losses of an investment – without taking potential profits into account. Therefore, they can be categorized as shortfall-oriented views of risk.

The often-used definition of risk by Boehm (1991, p. 33) also focuses on avoiding losses: "Risk exposure (RE) is the probability (P) of an unsatisfactory outcome (UO) times the loss (L) to the parties if the outcome is unsatisfactory". This definition matches the definition given by Cunningham (1967, p. 84) and contains a mathematical formulation which states that risk is the product of an occurrence probability and the amount of potential losses:

$$RE = P(UO) \cdot L(UO) \tag{2.1}$$

Another shortfall-oriented risk measure is the Value-at-Risk which will be introduced in section 4.1.3. Eckert (2006, p. 16) also describes risks from the shortfall-oriented perspective because she defines risks as the occurrence probability and amount of damages or losses.

Related to economic decision theory, risk is related to the knowledge of probabilities and probabilistic distributions in regard to future, uncertain events (Wolke, 2008, p. 1). This deviation from the expected value could be measured by characteristics such as the standard deviation σ or the variance σ^2 of the distribution. These measures incorporate positive as well as negative deviations from the expected value and the risk is considered to be higher when the deviation increases (Prokein, 2008, p. 7).

More risk-related characteristics will be presented in section 4.1.3. The relations between various risk-related terms, such as "attack", "vulnerability", and "threat", are shown in section 3.1.2 in figure 3.2.

2.2.2 The Nature of Perceived Risk as Multi-Dimensional Construct

Based on Cunningham (1967), perceived risk is commonly thought of as the feeling of uncertainty regarding the possible negative consequences of adopting a product or service and has formally been defined as the expectation of losses associated with a purchase. Additionally, perceived risk has been identified as important inhibitor to purchase behavior (e. g., Peter and Ryan, 1976). Perceived risk is especially relevant in decision-making when the circumstances of the decision create uncertainty, discomfort and/or anxiety, and conflict in the decision maker (Bettman, 1973). In various contexts, such as "acceptance of banking services" (Luo et al., 2010) or "intention to outsource business process" (Gewald and Dibbern, 2009), it has been shown that perceived risk has strong influence on the forming of attitudes and decision intentions (Ajzen and Fishbein, 1980; March and Shapira, 1987; Smith, 1992). A rich stream of literature showed that the assessment of risk is subject to various constraints related to the decision maker, leading to overestimation of risks (e. g., Gigerenzer, 2004; Gregory and Mendelsohn, 1993; Slovic, 1987) and underestimation of risks, i. e., "unrealistic optimism" (e. g., Rhee et al., 2012).

In line with Featherman and Pavlou (2003, pp. 453f.) and Gewald et al. (2006, p. 81), we define perceived risk as "the potential for loss in the pursuit of a desired outcome". The perceived severity of a risk rises with increasingly negative consequences or with decreasing control over the consequences (Koller, 1988, p. 267). This is consistent with the mathematical definition of risk by Boehm (1991, p. 33) and Cunningham (1967, p. 84), who define risk exposure as the product of probability of an unsatisfactory or undesirable outcome and the loss to the parties affected if the outcome is unsatisfactory or undesirable (see equation (2.1)).

Featherman and Pavlou (2003, pp. 454f.) typifies the overall perceived risk as having five dimensions that are related to (1) performance, (2) financial, (3) time, (4) psychological/social, and (5) privacy. Individual consumer's perceived risk as well as the risk perceived at the organizational level have been found to consist of multi-dimensional risk factors that affect product and service evaluations (e. g., Brooker, 1984; Kim et al., 2008; Bansal, 2011).

2.2.3 IT Risk Management Process

With great consistency, existing literature usually describes the risk management process as a cycle model consisting of four phases (e. g., Faisst et al., 2007, p. 513; Mitschele, 2008, p. 31; Prokein, 2008, pp. 15f.; Wolke, 2008, pp. 3–5; Beinhauer and Filiz, 2009, p. 91; Buxmann and Ackermann, 2010, p. 14): identification, quantification, treatment, as well as review and evaluation. For a more detailed process with seven phases see, e. g., Wheeler (2011, p. 46). An overview and comparison of nine different risk management approaches is given by Schlaak et al. (2008). In the following sections, the common four phases of the IT risk management process are discussed in more detail.

2.2.3.1 Risk Identification

The risk identification phase should result in the definition of relevant IT risks as well as the categorization of existing threats (i. e., risk sources). In order to determine these business-related threats, decision makers are required to identify possible vulnerabilities in their specific IT systems. Only after obtaining knowledge of the weak points, it becomes possible to determine which threats can exploit them and, thus, are relevant for risk management (Prokein, 2008, p. 16).

For the identification of IT risks, companies can employ various available methods that can be categorized into collection methods, creativity methods, as well as analytical search methods. Collection methods, such as checklists or expert interviews, have the risk-specific data collection in common. Therefore, they are mainly suitable for the identification of already known IT security risks. Creativity methods such as, brainstorming or the Delphi method, are based on creative processes, which are characterized by divergent thinking. Thus, they can be used to anticipate future previously unknown risks. Analytical search methods use the existing IT infrastructure and its characteristics as a starting point for searching vulnerabilities and threats (Prokein, 2008, pp. 19f.). Examples for these methods are threat or attack trees (Amoroso, 1994, pp. 15–29), or penetration tests (Eckert, 2006, pp. 76–86).

Reports from security-related organizations addressed IT security risks related to Cloud Computing. These reports can be used during the risk identification phase as checklists in order to discover more threats and risks in the individual scenario. For example, the Cloud Security Alliance provides guidelines and practical recommendations for managers that aim to protect security, stability, and privacy when using Cloud Computing (Cloud Security Alliance, 2011). Additionally, the Cloud Security Alliance issued a whitepaper including in-depth descriptions of the top

seven threats to Cloud Computing (Cloud Security Alliance, 2010). Likewise, the European Network and Information Security Agency (ENISA) also published recommendations regarding information security risks for potential and existing users of Cloud Computing (European Network and Information Security Agency, 2009). The report describes major risks, and presents an information assurance framework including technical measures for risk mitigation and provides guidelines regarding the assessment of security risks and benefits involved in the use of Cloud Computing.

A considerable amount of literature has been published on the risks related to ITO and classifications for related risks and challenges are discussed in various publications[1]. Earl (1996) discusses risks of traditional ITO, such as the possibility of hidden costs, business uncertainty, outdated technology skills, loss of innovative capacity, and technology indivisibility. Comprehensive reviews of literature on ITO are published by Dibbern et al. (2004) as well as Willcocks et al. (2007). A review of the ITO and Application Service Provision (ASP) literature is given by Lacity et al. (2009). They reviewed 34 published papers on ITO risks and risk management and list the 28 commonly mentioned risks. Major risks are contract, security, or privacy breaches by the vendor, poor capability or service, lack of trust, and vendor lock-in due to high switching costs. Methods for ASP risk mitigation are presented in Kern et al. (2002b). Mullender (1993) discusses the risks of distributed systems, consisting of processing elements and the communication networks, which can both fail or be attacked. The overall, distributed system offers more possibilities of interference, compared to in-house systems with their smaller attack surface. The failure of a single, central service might lead to the whole system's breakdown. More recent publications address business-oriented and service-specific threats in the context of the Internet of Services in which characteristics, such as loose coupling, composability and intermediary market places, are exploited (Miede et al., 2010a).

The quality of the results of the risk identification phase has a significant influence on the further phases of the IT risk management process. Since risk identification is an ex-ante analysis, there is always an inherent risk that not all business-related vulnerabilities, threats, and risk identified. Therefore, deficient and incomplete risk identification can result in additional, unanticipated losses for the company.

[1] Compare, in the following, Ackermann and Buxmann (2010); Ackermann et al. (2013).

2.2.3.2 Risk Quantification

The quantification of the identified IT-related risks is used to estimate to what extent these risks can endanger the achievement of corporate goals. Usually, the level of risk is determined by the parameters occurrence probability (i. e., the frequency of losses) and the amount of potential losses (i. e., the severity). An important characteristic of risk quantification is that it is referring to future events. Therefore, the phase always deals with imperfect information about the characteristics of the two risk-related quantities. Additionally, it is difficult to extrapolate these variables based on collected historical data because attacks and security measures change quickly due to rapid technological improvements (Prokein, 2008, pp. 16f.). For this reason, often multiple methods are used to estimate the loss frequency and severity. The accuracy of the results strongly depends on the quality, quantity, and topicality of the underlying data and information. Often used methods include scorecard-based reports, expert interviews, self assessments, as well as stochastic and causal methods (Faisst et al., 2007, pp. 514f.).

IT risk quantification methods in the form of metrics and risk measures for IT security have been examined only recently[2]. The Return on Security Investment (ROSI) is derived from the classic Return on Investment (ROI) which represents the financial gain of a project in relation to its total cost. ROSI measures the effect of risk mitigation in relation to a security measure's costs (Sonnenreich et al., 2006). Pinto et al. (2006) use a risk-based ROI which distinguishes between incident types and incorporates bypass rates to determine costs and benefits of security solutions. For a number of particular risks, formulas have been proposed to quantify the related losses. Patterson (2002) presents a formula for the estimated average cost of one hour of server downtime. Dübendorfer et al. (2004) define metrics for large scale Internet attacks, including downtime related loss, the loss due to disaster recovery, and liability cost which incur because contracts with third parties cannot be fulfilled and these third parties demand financial compensation. A risk model that is related to service networks is presented by Pang and Whitt (2009). They analyze service interruptions in large-scale service systems and quantify the impact of service interruptions with increasing scale of the systems. A survey of further economic security metrics is given by Böhme and Nowey (2008).

There is also a body of literature based on more complex quantification approaches regarding IT security investments. These publications, however, are not focused on systems, where Cloud Computing is used. Gordon and Loeb (2002) present an economic model which derives an optimal level of information security spending to protect a given set of information. Their model incorporates the vulnerability of information to a security breach and the potential losses resulting if

[2] Compare, in the following, Ackermann and Buxmann (2010); Ackermann et al. (2013).

such breaches occur. Wang et al. (2008) introduce the concept of Value-at-Risk in order to measure the stochastic behavior of daily losses due to security exploits. By using a Value-at-Risk approach they consider extremal yet perhaps relatively rare incidents and allow decision makers to make investment choices based on their own risk preference.

2.2.3.3 Risk Treatment

Based on the quantification of risks, the risk treatment phase aims at making decisions about how to deal with these risks. For this purpose, various approaches, such as risk reduction using technical countermeasures or transfer of risks using insurances by third parties, are available. Boehm (1991, p. 34) specifies three possible strategies for risk treatment, i. e., risk reduction, risk avoidance (through complete reduction of the probability and/or the potential losses), and risk transfer (e. g., to insurance companies). Often, decision makers face the problem to economically evaluate all possible measures as this requires a comparison of the effects of a measure (i. e., the reduction of future expected losses) and its implementation costs for taking action (Prokein, 2008, p. 17).

The effects of certain security measures can be evaluated through qualitative analysis of all risks, e. g., in the form of a risk exposure matrix (Wheeler, 2011, pp. 114f.), where all risks are placed based on their likelihood and severity. Those serious risks with higher ratings have to be treated before the medium- or low-level risks.

Eckert (2006) contains examples of security strategies as well as security architectures. The book provides detailed technical descriptions related to risk treatment in the fields of security models, cryptographic methods, signatures, key management, authentication methods, access control, and network security measures.

A number of recent, Cloud Computing-related reports provide guidance for risk treatment. A discussion of minimum security requirements for Cloud Computing providers can be found in Bundesamt für Sicherheit in der Informationstechnik (BSI) (2010). More technical, operational security guidance in Cloud Computing-related domains such as virtualization, data center operations, or encryption and key management is described in Cloud Security Alliance (2011).

Existing IT risk management literature provides several approaches that support IT security-related investment decisions during the phase of risk treatment[3]. A more formal approach in the field of decision support when taking measures is proposed by Faisst and Prokein (2005). They present a mathematical optimization model that helps decision makers determine the optimal amount to be invested in

[3] Compare, in the following, Ackermann and Buxmann (2010); Ackermann et al. (2013).

technical countermeasures (i. e., risk reduction) and insurance policies (i. e., risk treatment). Soo Hoo (2000) proposes a modeling approach that involves uncertain bad events causing losses and security countermeasures. He uses a decision analysis approach to evaluate a set of different levels of information security. Dutta and Roy (2008) developed a system dynamics model of the interplay between technical and behavioral security factors. They study the patterns in the value of an organization's IT over time in order to quantify the impact of security mechanisms. Based on stock-flow models for the user reaction sector as well as the organizational reactions associated with information security, they analyze responses to standard input test patterns. A game theory model is presented by Cavusoglu et al. (2004a). The model can be used to find the most cost effective configuration for intrusion detection systems based on the probability of intrusions and the costs occurring each time the organization manually monitors the audit trail for a possible intrusion. The application of real options techniques to information security is shown by Herath and Herath (2008). They propose a model which incorporates active learning and postauditing and can be used for the assessment of the value of information security assets and for the evaluation of investment decisions. Further risk mitigation approaches and strategies are described by Wheeler (2011, pp. 154–162).

With respect to Cloud Computing and the phase of risk treatment, specific methods with which it is possible to objectively assess and evaluate different countermeasures are missing. The phase of risk treatment offers possibilities for adjusting the security level of an IT scenario to state of the art measures and practices (Amoroso, 1994, p. 349). For example, it is possible to support risk treatment by providing lists of security measures that map Cloud Computing-related risks to applicable preventive actions. However, countermeasures should always be used in an economically reasonable way. As it is almost impossible (i. e., associated with high financial costs) to reach 100% security (Wheeler, 2011, p. 21), decision managers need to weigh the trade-off between increased security and the costs involved for the countermeasures. Additionally, security controls may also introduce new complexities to an environment (Wheeler, 2011, p. 11).

2.2.3.4 Risk Review and Evaluation

The IT risk management process is concluded by the risk review and evaluation phase that is sometimes called "risk monitoring" (Schlaak et al., 2008, p. 4). During the former three phases, i. e., risk identification, quantification, and treatment, an ex-ante view of IT risks has been made. On the contrary, the risk review and evaluation phase serves to control the ex-post analysis of the occurred losses

and the critical evaluation of the assumptions and decisions made in the previous phases.

Moreover, the duties of the control phase include ongoing reporting to different stakeholders, such as regulatory authorities as well as responsible persons in the company's management.

IT risk management does not generally only occur once. Instead, it is a continuous process, as the tools of the attackers, but also the available security technologies constantly evolve (Faisst and Prokein, 2005; Prokein, 2008).

2.3 Risks in the Context of IT Outsourcing and Cloud Computing

The analysis of risks related to different forms of Outsourcing has a long history in IS research and was merely done in studies that contrasted these risks with the opportunities in order to explain Outsourcing decisions. It is observable that the focus on specific risk dimensions changed over time and with the object of study – for example research on risks related to traditional IT outsourcing has tended to focus on strategic and financial risks rather than IT security in detail. With the rise of ASP and Cloud Computing the focus of the respective studies moved more and more in the direction of risks related to IT Security (see tables 2.1 and 2.2).

Early studies on IT outsourcing, such as, e. g., Quinn and Hilmer (1994), focus on the major strategic costs and risks of IT outsourcing and identify "loss of critical skills or developing wrong skills"; "loss of cross-functional skills"; "loss of control over a supplier". Loh and Venkatraman (1995) investigate how benefits and risks can serve as determinants of performance for IT outsourcing using a survey among 159 Chief Information Officers (CIOs). In 1996, Earl identified eleven risks associated with outsourcing IS services and distinguishes organizational, technical and operational, economic, and strategic risks. Bahli and Rivard (2003) propose a scenario-based conceptualization of IT outsourcing risk is and in a follow-up study, they suggest that client, supplier, and transaction are the three major sources of risk factors for IT outsourcing based on transaction costs theory (Bahli and Rivard, 2005). Aubert et al. (2005) propose a framework for the management of IT outsourcing risk, and validate the framework using data gathered in five case studies. Based on a literature review, they identify the main undesirable outcomes that may result from an IT outsourcing decision. Gewald and Dibbern (2009) analyze the factors that form an organization's attitude towards external procurement as well as its intention to adopt outsourcing. Based on the framework of Cunningham (1967), they identify financial, strategic, performance and psychosocial risk and model the adoption of outsourcing based on a risk-benefit analysis. In an extensive literature review on IT outsourcing, Lacity et al. (2009) identify 28 different risks related to IT outsourcing and discuss practical implications of those risks. These risks include, e. g., "breach of contract by the vendor", "cultural differences between client and supplier"; "excessive transaction costs"; "loss of autonomy and control over IT decisions"; "vendor lock-in", and also the risk of "security/privacy breech".

In the context of ASP, Jayatilaka et al. (2003) list 15 factors that explain the ASP choice – various of these factors can be considered as potential risks (or potential undesired outcomes), such as, e. g., "knowledge risk", "(insufficient) security of ASP", "(insufficient) ease of modification of the application", "(insuffi-

cient) compatibility with existing infrastructure". Currie et al. (2004) propose 28 Key Performance Indicators (KPIs) for potential ASP customers – the underperformance regarding those KPIs can be interpreted as "undesired outcome" – and reports that (based on a survey) the top KPIs are "data security and integrity"; "disaster recovery, back-up and restore"; "Service Level Agreements (SLAs)"; "financial stability of vendor"; "concentration on 'core' activities".

With regard to Cloud Computing, Armbrust et al. (2010) take a more technical perspective and identify three obstacles for adopting Cloud Computing solutions, five obstacles for the growth of Cloud Computing, and two policy- and business-related obstacles. Benlian and Hess (2011) study the opportunities and risks associated SaaS perceived by IT executives at adopter and non-adopter firms. The results of their survey indicate that for SaaS adopters as well as non-adopters, security threats are the dominant factor influencing IT executives' overall risk perceptions.

With the advent of new types of outsourcing (i. e., ASP and Cloud Computing), IT security risk became the most salient perceived risk dimension and get increasingly relevant for IS research – nevertheless, no comprehensive conceptualization of this construct exists and current studies were limited to simple and high-level conceptualizations with various and heterogeneous indicators (e. g., Chellappa and Pavlou, 2002; Flavián and Guinalíu, 2006; Casalo et al., 2007; Kim et al., 2008; Pavlou et al., 2007). Therefore, we propose and empirically validate a conceptualization of "perceived IT security risk" (PITSR) in the context of Cloud Computing in chapter 3 as part of our evaluation of perceived IT security risks.

Table 2.1 Selected Studies on the Risks of IT Outsourcing and Business Process Outsourcing

Study	Focus of the Study (related to Risk)	Identified / Discussed Risks
Research Area: Information Technology Outsourcing / Business Process Outsourcing		
Quinn and Hilmer (1994)	Comparison of IT outsourcing related strategic benefits and risks	"Loss of critical skills or developing wrong skills"; "loss of cross-functional skills"; "loss of control over a supplier"
Loh and Venkatraman (1995)	Analysis of risks as explanatory factors for outsourcing decisions	"Control risk"; "opportunism risk"
Earl (1996)	Identification of risks related to outsourcing	"Possibility of weak management"; "inexperienced staff"; "business uncertainty"; "outdated technology skills"; "endemic uncertainty"; "hidden costs"; "lack of organizational learning"; "loss of innovative capacity"; "dangers of an eternal triangle"; "technological indivisibility"; "fuzzy focus"
Bahli and Rivard (2003)	Scenario-based conceptualization of risks related to IT outsourcing	"Lock-in"; "contractual amendments"; "unexpected transition and management costs"; "disputes and litigation"
Aubert et al. (2005)	Identification of eight types of possible undesirable outcomes of IT outsourcing	"Unexpected transition and management costs"; "switching costs"; "costly contractual amendments"; "disputes and litigation"; "service debasement"; "cost escalation"; "loss of organizational competency"; "hidden service costs"
Bahli and Rivard (2005)	Identification of risk factors for IT outsourcing and development of a respective measurement scale	"Asset specificity"; "small number of suppliers"; "uncertainty"; "relatedness"; "measurement problems"; "(insufficient) expertise with the IT operation"; "(insufficient) expertise with outsourcing"; "(insufficient) expertise with the IT operation"; "(insufficient) expertise with outsourcing"
Gewald et al. (2006); Gewald and Dibbern (2009)	Identification of risks (based on the framework of Cunningham, 1967) related to Business Process Outsourcing	"Financial risk", "performance risk", "strategic risk", "psychological risk"
Lacity et al. (2009)	Review of IT outsourcing-related literature and identification of the most common discussed IT outsourcing risks	Identification of 28 risks, such as "breach of contract by the vendor", "cultural differences between client and supplier"; "excessive transaction costs"; "loss of autonomy and control over IT decisions"; "vendor lock-in"; "security/privacy breech"

Table 2.2 Selected Studies on the Risks of Application Service Provision and Cloud Computing

Study	Focus of the Study (related to Risk)	Identified / Discussed Risks
	Research Area: Application Service Provision (ASP)	
Kern et al. (2002c)	Identification of IT outsourcing risks and comparison of these risks between IT outsourcing and ASP	Identification of 15 risks, such as "unrealistic customer expectations"; "oversold supplier capability"; "supplier going out of business"; "incomplete contracting"; "supplier subcontracting problems"; "security breach"; "application unavailability"; "slow response time"
Jayatilaka et al. (2003)	Study of 15 factors to explain ASP choice	Key risks identified are "knowledge risk", "(insufficient) security of ASP", "(insufficient) ease of modification of the application", "(insufficient) compatibility with existing infrastructure"
Currie et al. (2004)	Evaluation of 28 KPIs for potential ASP customers (the underperformance regarding those KPIs can be interpreted as undesired outcome)	The top five rated KPIs are "data security and integrity"; "disaster recovery, backup and restore"; "Service Level Agreement (SLA)"; "financial stability of vendor"; "concentration on 'core' activities"
	Research Area: Cloud Computing	
Armbrust et al. (2010)	Identification of obstacles for Cloud Computing adoption and growth	"Availability/business continuity"; "data lock-in"; "data confidentiality and auditability"; "data transfer bottlenecks"; "performance unpredictability", "(problem of) scalable storage"; "(difficulties related to identify and remove) bugs in large distributed systems"; "(problems related to) scaling quickly"; "reputation fate sharing"; "(problems regarded to) software licensing"
Benlian and Hess (2011)	Analysis of salient risk dimensions of the perceived risk of SaaS adoption	"Security risk", "economic risks", "performance risks", "strategic risks", "managerial risks"

Chapter 3
Evaluation of Perceived IT Security Risks

In the course of this chapter, we develop a measurement scale for the Perceived IT Security Risk (PITSR) related to Cloud Computing[1].

> PITSR captures an organization's perception or attitude related to risks that are affecting the safety and security of a company's IT when Cloud Computing is used as a sourcing model.

On the basis of established scale development guidelines (Churchill, 1979; DeVellis, 2003; Hinkin, 1998; MacKenzie et al., 2011), we use a systematic five-step process, involving a variety of methods in order to develop, refine, and evaluate PITSR measurement. The process is completely bottom-up as we synthesize, refine, and evaluate the results of the explorative literature review in order to build an exhaustive and mutually exclusive taxonomy of IT security risks related to Cloud Computing. The dimensions and risk items are not predetermined top-down, but emerge during scale development and refinement. As shown in figure 3.1, the five steps were (1) a structured literature review in order to develop the initial measures, (2) the Q-sort method to refine the wording and to confirm the initial clustering of risks to risk dimensions, (3) qualitative interviews in order to further evaluate and refine the scale's measures, (4) construct conceptualization and model specification, and (5) the empirical survey to collect the data and to empirically validate the instrument.

[1] Compare, in the following, Ackermann et al. (2012).

T. Ackermann, *IT Security Risk Management,* DOI 10.1007/978-3-658-01115-4_3,
© Springer Fachmedien Wiesbaden 2013

Figure 3.1 Activities and Outcomes of the Five-Step Scale Development Process

3.1 Development of Measures Using a Structured Literature Review

A structured literature review was conducted in order to develop the content domain by generating our initial pool of risk items that represent the construct[2].

The literature review is based upon the approach described by vom Brocke et al. (2009). Hence, the procedure of excluding (and including) sources has to be made as transparent as possible. Moreover, the review should provide high validity and reliability in order to proof credibility. According to vom Brocke et al. (2009, p. 4), validity in this context is defined as "the degree to which the search accurately uncovers the sources". This involves the selection of scientific databases, keywords, and journals (Levy and Ellis, 2006). Reliability characterizes the "replicability of the search process".

Cooper et al. (2009) define a taxonomy of literature reviews which allows describing our methodology.

We focused on the research outcomes described or applied in the analyzed articles. Our goal was to integrate existing risk items into our work. We summarized and synthesized these items and took a neutral perspective. However, it is not possible to perform the selection of relevant risks completely neutral, as this extraction of technological risk items might be subjective to our interpretation. We tried to gain exhaustive coverage, but we were limited to those sources available for download by the seven chosen scientific databases. Our results are organized and arranged conceptually, so that works relating to the same items appear together. Our intended audience are IS researchers specialized in IT outsourcing or IT risk management, but our results might also be of value for other researchers in the IS community.

The following subsections describe our selection of sources and keywords with which we queried the databases.

3.1.1 Selection of Scientific Databases

For our collection of relevant publications, we used the following databases which taken together allow searching more than 3,000 business- and IT-related journals: EBSCOhost (with Business Source Premier (BSP) and EconLit databases), ISI Web of Knowledge (with Web of Science database) and Science Direct. We excluded Wiley Online Library and ingentaconnect as their usage would not have led to an increased coverage of top IS journals.

[2] Compare, in the following, Ackermann et al. (2011).

As our goal is to collect IT-related risks, we also queried the ACM Digital Library and the IEEE Xplore Digital Library as they cover the majority of publications from computer science disciplines. The AIS Electronic Library (AISeL) was used to cover the Journal of the Association for Information Systems (JAIS) as well as the proceedings of major IS conferences, such as European Conference on Information Systems (ECIS) and International Conference on Information Systems (ICIS).

This selection of scientific databases allowed searching the abstracts of 100% of the top 25 Management Information Systems (MIS) journals[3] and allowed accessing the full text of 92% of these ranked publications. However, some of them were only accessible after a certain delay and eight recent papers could not be downloaded because of these embargos.

We chose to query whole scientific databases without restricting the searches to specific journals or proceedings in order to gain high coverage of all relevant sources, to be as exhaustive as possible, and to find more risks. For the same reason, the queries were not restricted to a fixed time frame. We searched all covered years and did not exclude older papers.

3.1.2 Selection of Keywords

We were looking for papers in English language whose titles indicated that the publication is about IT outsourcing. Out of those, we were looking for papers that mention risk-related terms in either the title or the abstract.

The keywords were selected from the domains of IT outsourcing and IT security risks. To assure the quality of the keywords, the selection was done iteratively by sending test queries to the databases and by adding multiple synonyms and plural forms. For the terms related to IT outsourcing, we added commonly mentioned service models, and according acronyms, such as Cloud Computing, Software-as-a-Service, ASP, and SaaS. In conclusion, we queried the databases using the following keywords[4]:

[3] http://ais.affiniscape.com/displaycommon.cfm?an=1&subarticlenbr=432 [2012-03-14]

[4] The keywords “IS” and “IT” have only been used with scientific databases that do not treat “is” and “it” as stop words. We used hyphens whenever possible, e. g., to search for “Software-as-a-Service” as well as “Software as a Service”.

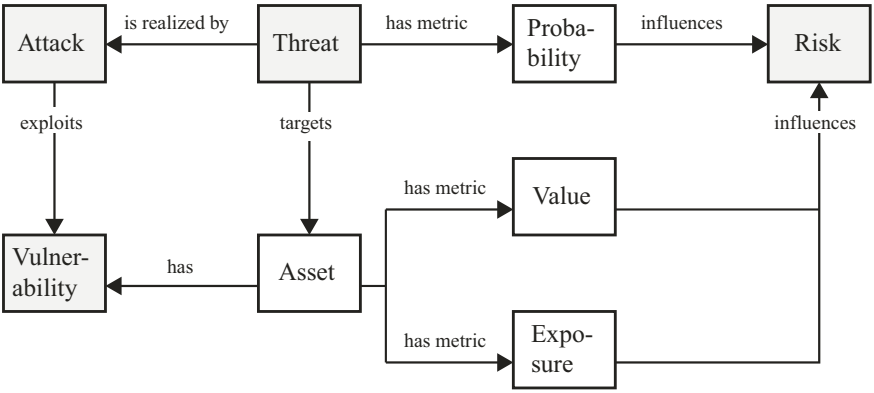


Figure 3.2 Relations between the risk-related terms "attack", "threat", "risk", and "vulnerability", based on Miede et al. (2010b).

```
( ( sourcing OR outsourcing OR outsource )
AND ( information-technology OR information-technologies OR
information-system OR information-systems OR service OR services
 OR application OR applications OR software OR IS OR IT ) )
OR
( cloud-computing OR software-as-a-service OR saas OR platform-
as-a-service OR paas OR infrastructure-as-a-service OR iaas OR
application-service-providing OR application-service-provider OR
 application-service-providers OR ASP OR netsourcing OR
esourcing )
```

Listing 3.1 Keywords related to IT Outsourcing

```
security OR safety OR risk OR danger OR weakness OR
vulnerability
OR attack OR threat OR risks OR dangers OR weaknesses OR
vulnerabilities OR attacks OR threats
```

Listing 3.2 Keywords related to Risk

Figure 3.2 provides the relations between some of the risk-related terms we used. Throughout this thesis, we use the term "risk" because especially from a risk management point of view, the metrics, associated with the threats and the affected assets, are important.

3.1.3 Search Filters

The search for papers with a title related to IT outsourcing and risk-related terms in title or abstract took place between May 28 and June 7, 2010, and resulted in 576 sources. We used further filters, such as searching for journals and proceedings only, papers with full text available, as well as exclusion of biology and chemistry journals. Application of these further search filters excluded 335 of the papers and, thus, reduced the set of relevant papers.

The resulting 241 papers identified by keyword search have subsequently been evaluated, based on their titles and other metadata, and later based on their abstracts, in order to assess their relevance for this study. 84 papers were out of scope and were therefore excluded.

Out of the remaining 157 papers, we were able to download 149. These have been evaluated based on a review of the whole content. This step resulted in exclusion of another 84 papers which were out of scope. Backward or forward searches were not part of our literature search strategy. Table 3.1 summarizes the steps done to reduce the number of relevant papers.

Finally, the search resulted in 65 final papers, which are listed in appendix A.1. The period covered by all 65 publications is 1993 to 2010, whereas 65% of all papers found have been published between 2007 and 2010. Content analysis of the final 65 papers resulted in 757 risk items.

3.1.4 Successive Refinement of Risk Items

In the following subsections, we describe the procedure used to successively refine the risk items and the taxonomy's dimensions. The method is comparable to the item sorting and grouping approach used by Ma et al. (2005, p. 1073).

Item Reduction

The high number of 757 initial risk items required us to reduce the number of items to a manageable set. Accordingly, as a first step, we merged items with same or similar meanings, e. g., "Poor response speed", "Low responsiveness", and "Unresponsiveness". By removing these duplicates, redundancy was reduced.

Table 3.1 The number of resulting papers after applying the search filters and after manual content filtering for each of the seven scientific databases.

	May/28 2010	May/28 2010	May/28 2010	May/28 2010	May/28 2010	May/31 2010	Jun/07 2010	
	ACM	EBSCO BSP	EBSCO EconLit	IEEE	Web of Science	Science Direct	AISeL	Total
A: Title is related to IT Outsourcing	105	2.220	109	612	3.542	724	70	7.382
B: Title is related to Risk	3.519	149.718	30.795	22.947	100.001	107.609	495	415.084
C: Abstract is related to Risk	12.123	589.510	56.605	83.591	n. a.	323.391	738	1.065.958
B OR C	13.122	631.609	73.403	87.307	100.001	376.688	1.122	1.283.252
A AND (B OR C)	12	267	5	84	153	50	5	576
Further Search Filters	10	31	1	81	71	42	5	241
Filter By Title and other Metadata	10	31	0	81	71	42	3	238
Filter By Abstract	10	29	0	69	21	25	3	157
Papers available for Download	10	29	0	69	16	22	3	149
Review by whole Content	5	12	0	26	7	14	1	65

Regrouping of Items

In this step, we tried to cluster similar items into different dimensions in order to build a suitable taxonomy. We iteratively moved the risk items from one dimension to another and added, renamed, or removed dimensions. This procedure led to new dimensions and concepts that we initially had not anticipated. The dimensions' names are chosen to match existing dimensions from IT security and quality of service literature. Table 3.2 lists the sources for each risk dimension.

Rarely referenced items that are subtypes of other items were also merged. For example, the items "Misuse services for sending spam" and "Misuse services for phishing", with one source each, were merged because they are more concrete instances of the item "Identity theft", i. e., the misuse of compromised credentials. Thereby, we decreased the items' redundancy.

The step of regrouping items was repeated multiple times. For four iterations, we invited other IS and computer science experts into different regrouping stages

Table 3.2 Sources for the Risk Dimensions

Source	Confidentiality	Integrity	Availability	Performance	Accountability	Maintainability
Gouscos et al. (2003)	✓	✓	✓	✓	✓	
Avižienis et al. (2004)	✓	✓	✓			✓
Carr et al. (1993)				✓		✓
Olovsson (1992)	✓	✓	✓			
Landwehr (2001)	✓	✓	✓		✓	
Álvarez and Petrović (2003)	✓	✓	✓		✓	

in order to achieve a gradual improvement of the clusters and to get feedback from different research backgrounds. In total, eight experts took part as coders in these regrouping sessions: Four IS or computer science researchers who hold a doctoral degree, three doctoral candidates researching on IT security in the context of Cloud Computing and one IS student.

After each iteration, we made sure, that the dimensions are exhaustive, i. e., that all items have been assigned to a dimension and that there are no items that do not fit into any of the dimensions. Furthermore, we analyzed the dimensions' intra-group homogeneity, i. e., that all items of a group are similar to each other. The initial pool of 39 risk items is shown in table 3.3, while tables A.1 and A.2 in appendix A.2 present detailed statistics on the sources (out of the 65 final papers of the literature review) for each risk item. Table 3.3 also contains the number of sources for each risk item (#S) as well as the number of individual sources mentioning at least one risk of a risk dimension.

The most frequently mentioned item ("Network performance problems") shows the literature's high level focus on the topic, while only a small amount of sources name specific attacks, such as eavesdropping or manipulation of transferred data.

It is remarkable, that only a small number of sources mention integrity-related risks (eight sources) because compromised integrity, for example, due to data modifications, can indirectly lead to a breakdown and downtime of a service. Likewise, risks related to accountability (14 sources), such as insufficient logging of performed actions and vulnerabilities in authentication and authorization mechanisms, may be causes of other more serious risks that are related with confidentiality, integrity, and availability. Risk items of the other four categories are mentioned by 31 to 37 sources. Furthermore, only "attacks" on integrity are discussed while

Table 3.3 Initial Pool of Items after the Literature Review

	Short Risk Item Description	#S
Confidentiality 34 sources	Supplier looking at sensitive data	18
	Compromised data confidentially	15
	Disclosure of data by the provider	12
	Insufficient protection against eavesdropping	7
	Eavesdropping communications	4
Integrity 8 sources	Data manipulation at provider side	5
	Accidental modifications of transferred data	3
	Manipulation of transferred data	3
	Accidental data modifications at provider side	2
Availability 37 sources	Discontinuity of the service	13
	Insufficient availability and low uptime	12
	Unintentional downtime	9
	Insufficient protection against downtime	7
	Service delivery problems	6
	Loss of data access	5
	Technical issues and system failures	5
	Attacks against availability	4
	Data loss at provider side	4
Performance 36 sources	Network performance problems	24
	Limited scalability	11
	Deliberate underperformance	8
	Insufficient service performance	7
	Insufficient protection against underperformance	4
Accountability 14 sources	Access without authorization	6
	Attackers generate costs	5
	Identity theft	5
	Insufficient logging of actions	3
	Insufficient user separation	3
Maintainability 31 sources	Incompatible with new technologies	17
	Inflexibility regarding business change	14
	IT becomes undifferentiated commodity	8
	Incompatible business processes	6
	Proprietary technologies	6
	Costly modifications are necessary	4
	Insufficient maintenance	4
	Limited customization possibilities	3
	Limited data import	3
	Service does not perfectly fit	2
	Unfavorably timed updates	2

#S: number of sources (out of the 65 final papers of the literature review) mentioning the risk

none of the sources discusses risks caused directly by compromised integrity, such as that the data may become unusable, files cannot be opened anymore, or that specific values in transmitted data (e. g., order quantities) are manipulated which might lead to false data in the planning systems.

Compared to the availability (nine risks) and maintainability (eleven risk) dimensions, fewer risk items are mentioned related to integrity, confidentiality, performance, and accountability. This is especially the case for performance risks, where 36 sources name only five different risk items.

The initial risk items developed in this section were further purified and refined using the Q-sort method and structured interviews with IT security experts.

3.2 Scale Evaluation and Refinement Using the Q-Sort Method

The Q-sort method is an iterative process in which the degree of agreement between judges forms the basis of assessing construct validity and improving the reliability of the constructs (Nahm et al., 2002). The process combines validation of content and construct through experts and/or key informants who group items according to their similarity. Furthermore, it also eliminates items that do not match posited constructs (Straub et al., 2004).

In each round, the judges were read short definitions of the six target dimensions. Then, they were asked to assign randomly shuffled cards with the 39 risk items to exactly one of the six target dimensions. This was done in order to test if all items can be assigned to exactly one of the existing dimensions. By doing so, we checked whether the dimensions are exhaustive and mutually exclusive, and whether the classification is unambiguous. We also asked the judges to name risks that are on another level of abstraction, i. e., to specific or to general, risks that could be merged together and risks where the assignment was difficult or unclear. After all cards were placed, the judges were told to check all assignments again and reorder cards if there was need to change.

After each of the three rounds performed, we calculated metrics described by Moore and Benbasat (1991) as well as Anderson and Gerbing (1991) in order to assess the validity of our categorization (see table 3.4). Therefore, we measured the percentage of judges that placed an item in the target dimension. This metric is also called "proportion of substantive agreement" and reported as "Average Item placement ratio" in table 3.4. For each dimension, we calculated the proportion of the target items that were correctly placed by the judges, i. e., the "class hit ratio". Additionally, we tested the inter-rater reliabilities by measuring the level of agreement between each pair of judges for each item. This metric is also called Cohen's Kappa (Moore and Benbasat, 1991).

After the first round of Q-sort, we merged 5 items, which were said to be similar by 4 of the 6 judges, into 2 new items. We also removed 5 items which were said to be too general by more than 2 judges. Furthermore, we rephrased all remaining items with an item placement ratio less than 80%, i. e., 13 out of our initial 39 risk items. The round ended with 31 items, thereof 2 merged and 13 reworded or new items.

During the second round of Q-sort, 2 items were said to be unclear or ambiguously formulated by 4 resp. 3 judges and therefore we rephrased these risk descriptions. Furthermore, we rephrased 3 remaining items with an item placement ratio less than 80%.

The third and last round of the Q-sort method showed that rephrasing did not increase the low placement ratios of two items, and thus we decided to finally drop

Table 3.4 Reliability Characteristics for each Round of the Q-Sort Method

Round	Average Item Placement Ratio	Average Class Hit Ratio	Average Cohen's Kappa
1st Round	72%	74%	68%
2nd Round	87%	87%	82%
3rd Round	91%	92%	86%
Final Risk Set	94%	94%	89%

them after two "rewordings". For four other rephrased items, the placement ratios became greater than 80% and they were therefore kept, according to the threshold proposed by Hinkin (1998) of a minimum ratio of 75%. The Q-sort step ended with 29 risk items in 6 dimensions, with average item placement and class hit ratios of 94%, and an inter-rater reliability of 89%. The detailed statistics of the Q-sort method are presented in appendix A.3 in tables A.3 to A.8.

Table 3.4 shows that the levels of agreement improved from round to round. After the three rounds of the Q-sort method, we analyzed certain attributes in order to evaluate the quality of the resulting taxonomy. According to Howard and Longstaff (1998), satisfactory taxonomies have classification categories with the following six characteristics.

- The taxonomy should be *exhaustive*, which means that all categories, taken together, include all the possible items: We queried seven scientific databases without restricting the searches to specific journals or time periods in order to identify as many relevant risk items as possible.
- The dimensions should not overlap (*mutual exclusiveness*). An important aspect of good taxonomies is that the taxonomy is clear and precise: We performed multiple rounds of clustering the initial set of items to dimensions – together with eight experts from different backgrounds – (see section 3.1.4) as well as the Q-sort method with six IS experts. We finally end up with six dimensions that are mostly free of overlaps (as shown by the high agreements in this and the following section). This aspect is also tightly related to the next characteristic.
- The classification should be *unambiguous*: Our last step, the final grouping with cards, was also conducted to make sure that the classification is certain, regardless of who is classifying. However, small limitations were found as there were items fitting into two categories. "Service delivery problems" and "Technical issues and systems failures", for example, could be classified as "Availability" and "Performance". In some cases, another reason for ambiguity exists as items that could be seen as cause and effect, such as "Insufficient maintenance" and

"Insufficient service performance", are grouped into different categories (maintainability and performance risks).

- Furthermore, repeated applications should result in the same classification, regardless of who is classifying (*repeatable*): We thoroughly documented the process of our literature review, and the intermediary steps to construct the taxonomy in order to reach high reliability. By incorporating participants with different backgrounds, we extracted categories with high intra-group homogeneity and high inter-group heterogeneity.
- The taxonomy's categories should be logical and intuitive, so that they could become generally approved and *accepted*: We used existing categories from IT security and quality of service literature (see table 3.2) and accordingly most categories are already approved by the research community.
- Finally, the taxonomy should be *useful* and lead to insight into the field of inquiry: To the best of our knowledge, this thesis provides the first collection and systematization of the technological risks of IT outsourcing. Additionally, in chapter 5, we show how the identified risk items can be practicably applied as part of the IT risk management process, in the phases of risk identification and in combination with an existing risk quantification model.

3.3 Scale Evaluation and Refinement Using Qualitative Interviews among Security Researchers

As it is important to aim for comprehensive coverage of items and avoid errors of omission during the conceptualization of the construct and scale development (Diamantopoulos, 2011, p. 354), we conducted qualitative interviews among 24 experts working on various fields of IT security (as PhD students or postdocs) ranging from cryptography to hardware security, trust and privacy to malware analysis. The interviews, which took around 16 minutes on average, also helped us to analyze the relevance of each measure, identify inappropriate or irrelevant items, and to improve understandability and coverage of the developed measures (Xia and Lee, 2005, pp. 18f.).

Following the process described by Homburg and Giering (1996, p. 14) as well as DeVellis (2003, p. 86), for each of the 29 risk items, we asked the experts whether the described risk is a) "obviously" b) "possibly" or c) "not" part of the target dimension. All items exceeded their proposed thresholds, i. e., at least 60% of the experts said that the item is obviously part of the dimension and at maximum 5% said that the item is not part of the dimension (see table 3.5). At most, one expert said that the item does not belong to the target dimension, which was the case for nine of the 29 risks. Detailed distributions of the experts answers to each risk item are shown in appendix A.4 in table A.9.

Table 3.5 Statistics of the Expert Interviews

Answer	Minimum	Average	Maximum
"obviously part of"	70.8%	87.2%	100.0%
"possibly part of"	0.0%	11.5%	25.0%
"not part of"	0.0%	1.3%	4.2%

Together with the experts, we discussed all risks and decided to remove 3 items related to security measures because – as the experts stated – they were redundant. We also asked whether some risks are hard to understand or descriptions might be ambiguous, which resulted in 7 rephrased items. For example, we rephrased some items to include data processing on remote servers instead of restricting the description to remote storage only.

Furthermore, in order to be as exhaustive as possible, we asked the experts if they know about dimensions and perceived IT security risks that we did not list. The experts confirmed the six dimensions and added five additional risk items:

- The risk that unauthorized persons can look at data on your internal systems (e. g., due to vulnerabilities of the browser or the used protocols).
- The risk that unauthorized persons modify data on your internal systems (e. g., through the interface to the provider).
- The risk that the availability of your internal systems is limited, e. g., during the data transfer to the provider.
- The risk that you experience performance issues of your internal systems (e. g., during the data transfer to the provider).
- The risk that actions can be performed on your internal systems (e. g., through the interface to the provider) which cannot be accounted to the initiator.

Those items are related to risks that occur in internal in-house systems instead of risks that occur at the side of the Cloud Computing provider. While the Q-sort procedure (see section 3.2) helped us to make sure that all items belong to the designated dimension, the interviews helped us to affirm another important aspect of content validity, i. e., that each risk dimension is exhaustively covered by its individual risk items.

Table 3.6 shows the number of risk items after each stage of the scale evaluation and refinement process. For each stage, we list the number of items added and removed, as well as how many risk descriptions were rephrased. After the expert interviews, we ended up with the final 31 risk items which were used in the survey (see tables A.10 and A.11 in appendix A.5 for the exact wording of the final risk items).

Table 3.6 Number of Risks after each Stage of the Evaluation and Refinement Process

Step	Risks	Added	Removed	Rephrased
Literature Review	39	-	-	-
Q-Sort Round 1	31	-	5+3	13
Q-Sort Round 2	31	-	-	6
Q-Sort Round 3	29	-	2	-
Expert Interviews	31	5	3	7

3.4 Construct Conceptualization and Model Specification

This section is divided into two parts. First, the multi-dimensional measurement model is formally specified in section 3.4.1. Then, in section 3.4.2, the developed six security risk dimensions are described in more detail.

3.4.1 Formal Measurement Specification

An important step in scale development is to formally specify the measurement model and the directions of causality for the indicators and constructs. In line with previous studies on risk perception that already included sub-scales and multiple risk dimensions (Peter and Tarpey, 1975; Havlena and DeSarbo, 1990; Mitchell and Greatorex, 1993; Featherman et al., 2006; Benlian and Hess, 2011), and the guidelines for conceptualizing multi-dimensional constructs in IS research (Polites et al., 2012), we model the aggregated perceived IT security risk as a multi-dimensional construct.

Owing to the fundamental differences of reflective and formative measurement, possible misspecifications should be avoided (Jarvis et al., 2003; Petter et al., 2007; Bollen, 2011). While reflective indicators are affected by an underlying latent, unobservable construct, formative constructs are a composite of multiple measures (MacCallum and Browne, 1993, p. 533). Reflective and formative measures have different strength and weaknesses, such as parsimony versus richness, generality versus precision, and few versus many items, respectively (Barki et al., 2007, p. 178). In order to decide how to model the relationship between the identified risk items and the risk dimensions, we applied the decision rules given by Jarvis et al. (2003, p. 203). All four rules called for formative measurement, which is in line with the mathematical definition of risk, where a risk is the product of probability of an unsatisfactory event and the potential losses which could be caused by the event (see, e. g., Boehm, 1991, p. 33 and equation (2.1)), and where multiple independent risks can be summed up to a total, aggregated risk value:

1. Changes in the indicators should cause changes in the construct but not vice-versa. This means that the direction of causality is from the individual risk items to the risk dimension and all indicators of a risk dimension are the defining characteristics of this construct. If a single risk item is perceived stronger, the aggregated construct score should also reflect this increase. On the contrary, a higher score of a risk dimension does not mean that all its indicators are perceived more risky.

2. It is not necessary for indicators to covary with each other. The availability-related risk that "it comes to unintentional downtime, e. g., because of technical errors and system crashes" can be perceived to be very serious while another risk in the same dimension, such as the risk that "the provider experiences data loss and the data may not be recoverable", can be perceived completely different.
3. Indicators are not interchangeable and do not have similar content. We carefully selected and refined the risk items so that they have as little overlap as possible while still covering all relevant aspects of a risk dimension. Therefore, dropping a single indicator may alter the conceptual domain of the construct and the risk items' exhaustiveness would decrease.
4. Indicators are not required to have the same antecedents and consequences. Some of our individual risks may be perceived to be more serious after a recent security incident while the perception of other risks in the same dimension does not necessarily change.

The identified risk sub-dimensions are viewed as defining characteristics of the focal construct, the aggregated perceived IT security risk related to Cloud Computing. Analog to the formative view of individual risk items to our risk dimensions, the decision rules of Jarvis indicate that the sub-dimensions are formative indicators of the second-order focal construct. Therefore, we treat PITSR, our focal construct, as a function of its sub-dimensions and in summary, the resulting construct structure is classified as a formative first-order, formative second-order model ("type IV" as it is called by Jarvis et al., 2003, pp. 204f.). In this type of model, the dimensions are combined and aggregated to form the overall representation of the construct, and the indicators of each dimension likewise form their respective dimensions (Polites et al., 2012, p. 30). The used form of an aggregate additive model allows that each dimension of perceived risk contributes separately to the meaning of the construct and might be differentially weighted. Unlike previous studies that treated security related risks as simple, one-dimensional measures (e. g., Chellappa and Pavlou, 2002; Flavián and Guinalíu, 2006; Casalo et al., 2007; Kim et al., 2008; Pavlou et al., 2007), we propose a more complex construct that captures aspects and relationships that have not been included before.

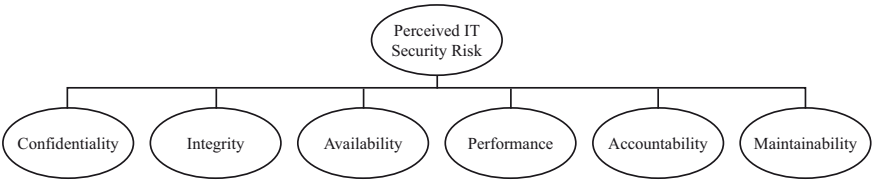


Figure 3.3 Dimensions of Perceived IT Security Risk

3.4.2 Descriptions of Security Risk Dimensions

Information security is a highly dynamic field of action that follows the technical development. The various safety objectives have been developed in parallel over time[5]. Twenty years ago, security was virtually set equal to confidentiality, while fifteen years ago, integrity and availability joined. About ten years ago, accountability, the fourth objective of protection, was added (Roßnagel et al., 2001, p. 229). Nowadays, numerous other safety objectives, such as accountability and maintainability are widely acknowledged.

The proposed taxonomy of IT security risks related to Cloud Computing is shown in figure 3.3. The dimensions are named after attributes or qualities of information and IT security. At the same time, these attributes are goals of protection which companies should seek to defend as part of their IT risk management process. All security risks in a given dimension negatively affect the safety objective that gave the name to the corresponding dimension. The sources for the names of each dimension are listed in table 3.2.

In the following six sections, the security dimensions developed based on the literature review and evaluated using the Q-sort method and expert interviews are described and exemplary risks and countermeasures are presented.

3.4.2.1 Confidentiality Risks

The confidentiality of an IT-system remains intact, as long as the information contained therein is accessible only by authorized users. This means that the safety-relevant elements become only known to a defined circle of people (Stelzer, 1993, p. 35).

Confidentiality risks include deliberate attacks that affect the privacy and confidentiality of the customer's data, such as eavesdropping communications (e. g.,

[5] Compare Bedner and Ackermann (2010) for some of the following descriptions of the security risk dimensions, individual risks, and countermeasures.

Jensen et al., 2009; Viega, 2009; Dawoud et al., 2010), as well as the risk that data are disclosed by the provider to unauthorized third parties (e. g., Itani et al., 2009; Kaufman, 2009; Viega, 2009). Possible insider attacks include, e. g., that employees of the supplier are looking at sensitive customer data stored or processed on their servers (e. g., Beulen et al., 2005; Briscoe and Marinos, 2009; Schwarz et al., 2009).

In order to protect confidential data, measures to define and control permitted information flows between the entities of the system are required (i. e., access control as well as access rights), so that it can be ruled out that information is "leaked" to unauthorized entities (Eckert, 2006, p. 9). Stored data should be encrypted, so that unauthorized persons cannot read the data. Transmitted data can be protected by using encrypted channels such as Secure Sockets Layer (SSL) connections or Virtual Private Networks (VPNs) (Kern et al., 2002b, pp. 93f.).

3.4.2.2 Integrity Risks

Integrity is given if data cannot be modified, e. g., manipulated, by unauthorized persons. Regarding Cloud Computing systems, integrity can also be defined as completeness and correctness of data (i. e., data integrity) in combination with correct functionality of the Cloud Computing system (i. e., system integrity). Completeness means that all pieces of information are available while correctness means that the data represent unaltered facts (Bedner and Ackermann, 2010, p. 326).

Integrity is compromised, whenever any unauthorized change to information in transmission, storage, or processing is involved (Amoroso, 1994). These changes range from systematic and intentional manipulation to unsystematic distortion and unintentional modification. Possibilities for systematic changes are replacement, insertion, and deletion of data, or parts thereof (Wang et al., 2009). For example, data transferred to the Cloud Computing provider can be manipulated using man-in-the-middle attacks if no or weak encryption is used (e. g., Dawoud et al., 2010; Jensen et al., 2009).

Frequently, checksums or fingerprints based on secure cryptographic hash functions, such as Secure Hash Algorithm (SHA)-2, are used in order to detect changes to the data (Eckert, 2006, pp. 353–387). Thereby, it is at least possible to avoid subsequent processing of the altered data.

3.4.2.3 Availability Risks

Availability means that users are able to access the service and the data whenever they want to. This means that the system has to be able to deliver services when they are requested (Sommerville, 2006). In contracts and SLAs, availability is often understood as the ratio of the time in which the system was actually available (i. e., the so-called "operation time") in a specified time frame which does not include maintenance periods. This ratio is often reported in percent and the period where a system was not available is often called "downtime" (Söbbing, 2006, pp. 409f.).

Deliberate attacks against availability (e. g., Bhattacharya et al., 2003; Jensen et al., 2009; Zhang et al., 2009) aim at the nonavailability of Cloud Computing services. This is commonly performed using Denial of Service (DoS) attacks over the network, where a server is flooded by requests in order to cause capacity overload. If the attack is carried out using many different, distributed attacking machines, it is called a Distributed Denial of Service (DDoS) attack (e. g., Dawoud et al., 2010, p. 5; Zhang et al., 2009, p. 130). Besides, natural disasters or technical failures may cause unintentional downtime (e. g., Aron et al., 2005; Benefield, 2009; Yildiz et al., 2009). When users are no longer able to log on to the service, they end up with no access to their data that are stored on remote servers of the Cloud Computing provider (Schwarz et al., 2009; Viega, 2009).

Commonly found countermeasures include the usage of redundant systems, including in-house backups of all data stored on the remote servers. At the side of Cloud Computing providers, load-balancing mechanisms, as well as packet filtering are used to protect the systems against DoS attacks (Dawoud et al., 2010, p. 5).

3.4.2.4 Performance Risks

If a Cloud Computing service is with good performance this denotes that the use of the service and the data take place in the speed that meets the customers' requirements. A major concern regarding IT outsourcing is underperformance because of technical network issues (Kern et al., 2002c). For example, the speed of delivery could be too low because of throughput problems, high response times, or bandwidth limitations (e. g., Kern et al., 2002a, pp. 156–158; Beulen et al., 2005, pp. 136 & 141; Ma et al., 2005, p. 1073).

Other risks that are especially relevant in the Cloud Computing context – as it makes heavy use of virtualization – are issues with scalability and elasticity of the provided services. These risks are related to situations when a user's intensity of use – or the overall usage – changes, especially increases (e. g., Kern et al., 2002a, p. 157; Briscoe and Marinos, 2009, p. 105; Brynjolfsson et al., 2010, p. 33).

In order to ensure performance, Cloud Computing providers should make use of load-balancing and operate redundant systems, including duplication of critical components such as hardware, power systems, and internal networking infrastructure (e. g., Walsh, 2003, p. 105; Ma et al., 2005, p. 1073). Additionally, providers should create frequent backups and use mirroring and distributed replication of stored data (e. g., Briscoe and Marinos, 2009, p. 106; Currie, 2003, p. 212).

Even before a Cloud Computing service is sourced, it is important to have contractual assurance of performance metrics in the form of Service Level Agreements (SLAs). The contracts should also contain clauses regarding breach of the contract by the Cloud Computing provider, including fines for poor delivery and performance (e. g., Patnayakuni and Seth, 2001, p. 182; Bahli and Rivard, 2005, pp. 178f.; Osei-Bryson and Ngwenyama, 2006, pp. 246f.).

3.4.2.5 Accountability Risks

Accountability remains intact if authentication mechanisms cannot be bypassed and when all actions performed in the course of using the service and the data can clearly be assigned to an identifiable user. Therefore, accountability risks are related to the problem of identifying, authenticating, and authorizing trusted users (Schneier, 2004).

A common accountability risk is that it is possible to access the Cloud Computing service and the data without proper authorization (e. g., de Chaves et al., 2010, p. 215; Mowbray and Pearson, 2009, p. 2). But even if authentication mechanisms cannot be bypassed, the risk of identity theft remains. This means that attackers that are in possession of login credentials (e. g., passwords) can perform actions in the system in the name of the actual owner. Moreover, it may be possible for them to generating costs in the name of legitimate customers (e. g., Goodman and Ramer, 2007; Jensen et al., 2009; Viega, 2009). By using secure cryptographic credentials such as one time passwords or digital certificates (e. g., Ying et al., 2008, pp. 1014f.) instead of simple passwords, Cloud Computing users can reduce the risk of identity theft.

Another accountability risk is related to the Cloud Computing concept of multitenancy, where a single software instance, running on a server, serves multiple users in parallel. If the users sharing a system are insufficiently separated from each other, it may be possible to perform actions on other users' virtual machines (e. g., Viega, 2009, pp. 106f.; Dawoud et al., 2010, pp. 3–5; de Chaves et al., 2010, p. 215). For example, poor separation could subsequently lead to confidentiality risk such as eavesdropping communications.

In order to protect the accountability, it is required that the performed actions can be interlinked and assigned to identifiable persons. For example, the account-

ability of system usage can be safeguarded by implementing authentication mechanisms for all users as well as by logging all performed actions in combination with digital signatures and trusted timestamps (Bedner and Ackermann, 2010, p. 325). If it is not possible to modify (i. e., manipulate) these log files, then non-repudiation is given. This means that users which performed logged actions cannot deny these actions (Zhou et al., 2008, p. 747).

3.4.2.6 Maintainability Risks

A Cloud Computing service is maintainable if it is possible to adapt the service to individual requirements, and when maintenance and support are ensured by the provider. Risks related to maintainability can affect a system's ability to undergo modifications or repairs (Avižienis et al., 2004). This includes integration of external systems, as well as the migration from and to another provider.

One of the major maintainability-related risks is that Cloud Computing providers often use non-standardized, proprietary interfaces to their services, thus, creating a lock-in for their users (e. g., Buyya et al., 2008, p. 11; Everett, 2009, p. 5; Weinhardt et al., 2009, p. 395; de Chaves et al., 2010, p. 215). Therefore, users should verify that the provider offers the possibility to export the data in an ideally open and interchangeable file format that will allow being imported to a substitute application (e. g., de Chaves et al., 2010, p. 215; Everett, 2009, p. 5).

Furthermore, because Cloud Computing services are offered on a one-to-many basis (i. e., multitenancy) they often only provide limited possibilities for customization. Therefore, the service cannot be flexibly be adapted to changes in business processes or the internally used in-house software (e. g., Kern et al., 2002a, pp. 157f.; Lu and Sun, 2009, p. 508).

Finally, there is the risk that the Cloud Computing provider insufficiently maintains the service and possibly realizes only few improvements. In extreme cases the provider could completely stop the further development of the service (e. g., Nakatsu and Iacovou, 2009, p. 61).

In order to reduce some of the maintainability-related risks, potential users should particularly pay attention to contracting issues before the Cloud Computing service is sourced. The contracts should be flexible in regard to renegotiation, price adjustments, termination of the contract, and shortening the contract period. (e. g., Bahli and Rivard, 2003, p. 217; Gefen et al., 2008). Additionally, the contracts should include penalties as well as termination clauses (e. g., Jurison, 1995, p. 245; Bahli and Rivard, 2005, p. 178). The Cloud Computing provider should be required to report incidents, and security breaches should be grounds for compensation and possible contract termination (Goodman and Ramer, 2007, p. 818).

3.5 Scale Assessment and Validation Using an Empirical Survey

3.5.1 Survey Development and Implementation

3.5.1.1 Pre-Testing the Questionnaire

To assess model constructs, a questionnaire was developed and pretested with doctoral students and three IS professionals, resulting in minor wording changes. We conducted cognitive interviews using think aloud answers to ensure face and content validity of the indicators and in order to avoid misunderstandings (Bolton, 1993).

Especially the pre-tests with the three professionals working in IT departments of German companies provided helpful feedback regarding wording issues. By identifying the respondents' difficulties arising during the response process, we assessed whether good translations of the constructs have been achieved.

However, since the developed items had already been intensively pre-tested, only minor changes were necessary and the remarks decreased steadily (from nine minor changes after the first pre-test, one reworded item after the second pre-test, and no changes after the third pre-test). The final form of the questionnaire is shown in appendix A.6.

3.5.1.2 Case Selection

The revised questionnaire was then distributed to 6,000 German companies, randomly drawn from the Hoppenstedt database (release Q3 2011). Hoppenstedt is one of the largest commercial business data providers in Germany. The database contains more than 300,000 profiles of German companies and contact persons within each company.

To support the external validity of our study, we did not constrain the sample to specific industries or to firms of a specific organizational size. Especially since SME are often said to be the target group of Cloud Computing (Marston et al., 2011, p. 184), we did not limit the study to only include the largest companies. We thus drew a random sample from the entire population of company profiles in the Hoppenstedt database.

The companies were contacted by mail and e-mail and the contacts within each company were not chosen on a random basis but because they have special qualifications such as particular status or specialized knowledge (Phillips, 1981, p. 396). We addressed the key informants in the following order of preference: Whenever possible, we contacted the companies' CIO. Especially for some smaller compa-

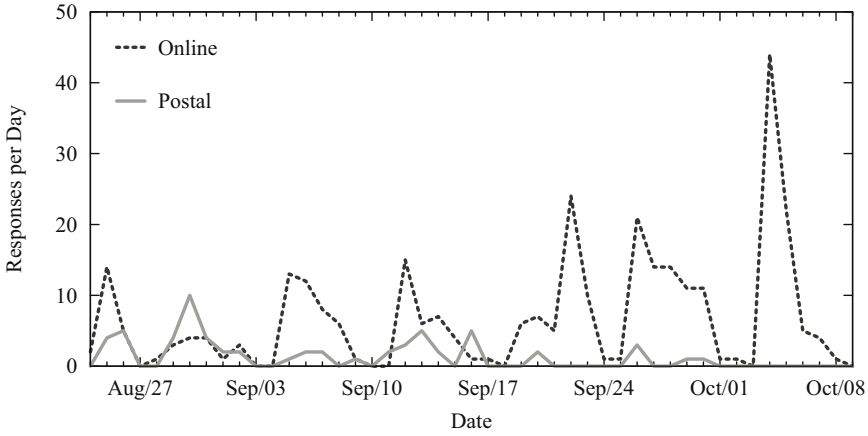


Figure 3.4 Completed Survery Responses over Time

nies only the Chief Executive Officer (CEO) was available, whom we contacted if the CIO was not specified. By contacting these key informants, we assume that the survey respondents provide information at the aggregate or organizational unit of analysis by reporting on group or organizational properties rather than personal attitudes and behaviors (Phillips, 1981, p. 396). Therefore, we used questions which ask for the company's perspective and emphasized that the respondents should answer the questions on behalf of their organizations.

The postal letters contained the questionnaire, a letter outlining the purpose of the research and soliciting the contact person's participation, as well as a postage paid return envelope. The cover letter also included a link to the identical online survey and an individual password for each company with which the online survey could be accessed.

In order to minimize response-set artifacts, the sequence of the indicators within each dimension was randomized (Andrews, 1984; Hilkert et al., 2011). We also used two versions of the printed questionnaire with altered ordering of the indicators.

3.5.1.3 Survey Schedule

The study took place between August, 22th and October, 9th 2011. Participation was encouraged by offering an individualized free management report comparing the individual answers against companies of the same industry, and by reminders

via mail. Additionally, we called around 2,750 out of the 6,000 randomly drawn companies.

The number of responses per day is shown in figure 3.4. It can be seen that there were almost no responses during the weekends and there was a downward trend within each week, i. e., most answers arrived on Monday and Tuesday, while there were less answers on Friday. Most participants (i. e., 314 fully completed questionnaires) used the online survey (dashed blue line), while only 61 answered via the postage-paid return envelopes (solid red line)[6]. Visibly more responses arrived shortly after our e-mail reminders on September, 5th and October, 4th, and when the postcard reminders send to the companies arrived around September, 22nd.

During the phone calls, we asked for the reasons, why some companies did not want to participate. Most often, the reason was that company policies forbid taking part in surveys (because of security reasons, or the respondent was too busy or received too many surveys). Some persons, working in IT departments told that they do not see themselves as the target group for Cloud Computing, mostly because the existing IT infrastructure is too small.

3.5.1.4 Sample Characteristics

A total of 472 questionnaires were received, representing a response rate of 7.87%. However, some of these responses had to be excluded from the sample due to missing data and low data quality. As we only used data sets without missing values, we excluded all questionnaires that were not fully completed by the respondents. Therefore, the results presented in this thesis are based on the final sample size of 356 valid responses. This response rate is low but still acceptable regarding the difficulties in obtaining survey responses from IS executives and corporate-level managers (Poppo and Zenger, 2002).

Although the comparison of the respondents' characteristics with those of the original target sample did not show major differences, we carried out a further investigation of a possible non-response bias. Following Armstrong and Overton (1977), we compared the first 25% and the late 25% of responses. Utilizing t-tests, none of the variables showed significant differences. Additionally, we performed a series of chi-square comparisons which also showed no significant differences between early and late responses. The two lowest Pearson chi^2 significances for

[6] Please note that 97 additional incomplete questionnaires arrived during the reported period which were not counted because of missing data. These incomplete responses are also not shown in figure 3.4.

Table 3.7 Survey Sample Characteristics

	Company Size
16%	Small businesses (<50 employees)
39%	Medium companies (50–249 employees)
45%	Large enterprises (>249 employees)
	Respondent Title
14%	Chief Executive Officer (CEO)
49%	Chief Information Officer (CIO)
11%	Head of IT department
17%	Employee in IT department
9%	Other

individual measures were 0.05 and 0.09, while the average significance was 0.585, indicating strong evidence that the two groups do not differ.

Table 3.7 shows that 63% of all respondents were CEO or CIO. Additionally, 84% of the respondents answered that they are directly responsible for the selection and decision regarding the considered type of application. Both statistics suggest that we were able to reach key informants in the responding companies.

Given the single method we had used to collect the data, we also conducted a series of tests in order to analyze Common Method Bias (CMB). Harman's one factor test using exploratory factor analysis (Podsakoff and Organ, 1986) resulted in 12 extracted factors, and the strongest component explained only 34% of the variance, which is less than the proposed threshold of 50%. Furthermore, we tested for CMB using a latent common method factor (Bagozzi, 2011, p. 277–282). At maximum 7% of the variance in our reflective and formative measures were explained by the latent method factor. Finally, we included a correlational marker variable[7] in our questionnaire (Bagozzi, 2011, p. 281f.) that fulfilled the criteria of good correlational markers: on average, it showed the smallest correlation with all other manifest measures. The maximum variance explained by the marker variable was 1.9%, while on average 1.37% of our reflective and formative measures' variance was explained. All tests suggest that CMB is unlikely to have significantly affected our analyses and results.

[7] Marker Variable: "The essential goal of our corporate strategy is to increase our customer service's quality."

3.5.2 Methods of Validation

We applied Covariance Structure Analysis (CSA) and employed LISREL (version 8.80; Jöreskog and Sörbom, 2006) as it is probably the most widely used software for CSA (Diamantopoulos, 2011, p. 336). While the Partial Least Squares (PLS) approach has several attractive features, its measurement model assumes that the focal construct is fully determined by its indicators. As we wanted to assess the disturbance terms of the constructs and analyze how well the indicators together explain a construct, we performed CSA. Furthermore, LISREL accounts for all the covariance in the data and provides more accurate parameter estimations than other techniques (Gefen et al., 2003).

In order to identify the models, we used one of the scaling methods proposed by Diamantopoulos (2011, p. 345), i. e., fixing the path from a latent variable (i. e., construct) to an outcome variable (i. e., a reflective indicator) to unity (as recommended by Bollen and Davis, 2009).

For the establishment of reliability and validity of our developed PITSR scale, which measures the perceived IT security risks related to Cloud Computing, we followed the validation guidelines provided by MacKenzie et al. (2011).

We used the Multiple Indicators, Multiple Causes (MIMIC) approach in order to achieve model identification (Diamantopoulos and Winklhofer, 2001; Diamantopoulos, 2011). The MIMIC approach requires that constructs having formative indicators, i. e., the dimensions of perceived IT security, are also assessed with appropriate reflective indicators. Consequently, two individual reflective indicators for each dimension were developed based on Featherman and Pavlou (2003). The respondents were asked to complete sentences such as the following: "Regarding the availability of your systems and data, it would be . . . for your company to use Cloud Computing". We used two semantic differentials in order to assess the perceived risk and the respondents were able to choose where their position lies on a 7-point scale between two bipolar adjectives, i. e., "not risky at all" – "very risky" as well as "associated with very little uncertainty" – "associated with great uncertainty".

As the focal construct, the aggregated perceived IT security risk, was not measured by any formative indicators, we added a third reflective measure based on Featherman and Pavlou (2003). The third semantic differential added the two bipolar adjectives "associated with little threats" – "associated with strong threats". Finally, we used the measurement model that can be seen in figure 3.5.

Table 3.8 Goodness of Fit Statistics of the Measurement Model

Statistic	Basic Model
N	356
chi^2	1,386
df	518
chi^2/df	2.676
GFI	0.842
RMSEA	0.075
SRMR	0.074
CFI	0.982
NFI	0.972
TLI	0.964

3.5.2.1 Evaluating the Goodness of Fit of the Measurement Model

As LISREL was utilized for the analysis of the MIMIC Structural Equation Model (SEM), we assessed whether the estimation procedure converges and none of the variance estimates are negative, i. e., whether the solution is "proper".

Likewise, we found significant critical ratios (i. e., paths) for the individual hypothesized constructs and indicators. These statistics related to individual indicators are discussed in detail in sections 3.5.2.4 to 3.5.2.6. With its 518 degrees of freedom (df), the model has a chi^2 statistic of 1,386 that is strongly significant (p=0.0). The chi^2/df ratio of 2.676 indicates a good model fit (Carmines and McIver, 1981; Wheaton et al., 1977). Consistent with established recommendations on the evaluation of LISREL estimation results, a number of absolute and relative fit indices were analyzed in order to evaluate the overall model fit.

Regarding the absolute fit of the model, we received mixed results: While the Standardized Root Mean Square Residual (SRMR) of 0.074 indicates good model fit, the Goodness of Fit Index (GFI) of 0.842 is below the commonly used threshold of 0.90. The Root Mean Square Error of Approximation (RMSEA) of 0.075 is slightly above the threshold of 0.06 proposed by MacKenzie et al. (2011, pp. 312f.), but still in an acceptable range (Browne and Cudeck, 1993, p. 144). However, due to the high model complexity (31+12+3=46 indicators and 7 latent variables) and the comparably low sample size of N=356, the results of the relative fit indices, which are less sensitive to sample size, should be considered (Hu and Bentler, 1999; Hilkert et al., 2011). Therefore, we also assessed the fit relative to a suitably framed comparison model and received decent fit statistics: The Comparative Fit Index (CFI) of 0.982 indicates a good model fit. Likewise, the

Table 3.9 Construct AVE, R^2, Alpha, and Reliability

Construct	AVE	R^2	Alpha	CR
Confidentiality	0.837	0.62	0.946	0.911
Integrity	0.907	0.48	0.968	0.951
Availability	0.777	0.51	0.916	0.875
Performance	0.858	0.55	0.946	0.924
Accountability	0.856	0.63	0.945	0.922
Maintainability	0.892	0.62	0.958	0.943
PITSR	0.725	0.59	0.901	0.887

Normed Fit Index (NFI) of 0.972 as well as the Tucker Lewis Index (TLI), also called Non-Normed Fit Index (NNFI), of 0.964 are all above the threshold of 0.95 proposed by Hu and Bentler (1999, p. 27). For these reasons, we concluded that our measurement model has an acceptable goodness of fit.

Table 3.8 shows the goodness of fit indices for the basic measurement model consisting of PITSR, the focal construct, as well as its six IT security risk dimensions and their MIMIC indicators.

3.5.2.2 Assessing the Validity of the Set of Indicators at the Construct Level

The convergent validity of the sub-dimensions was assessed by calculating the Average Variance Extracted (AVE) for our six first-order latent constructs. The AVE measures the average variance in the indicators that is accounted for by the focal construct, and its value should exceed 0.5 (Fornell and Larcker, 1981). Table 3.9 shows that the AVEs for all risk dimensions vary between 0.777 and 0.907, and clearly exceed the given threshold.

For first-order latent constructs with formative indicators it is not necessary to check for convergent validity, as the formative specification does not imply that the indicators should necessarily be correlated (MacKenzie et al., 2011, p. 313). Following Diamantopoulos et al. (2008, p. 1216), we used the magnitude of the construct level error term in order to assess the validity of the sets of indicators at construct level. The variance of the residual is smaller than the explained variance (R^2) for all formative constructs except integrity-related risks, where R^2 is 0.48 and zeta is 0.52. However, known groups comparison (see section 3.5.2.7 for more details) showed that R^2 for all groups exceeds the proposed threshold of 0.5

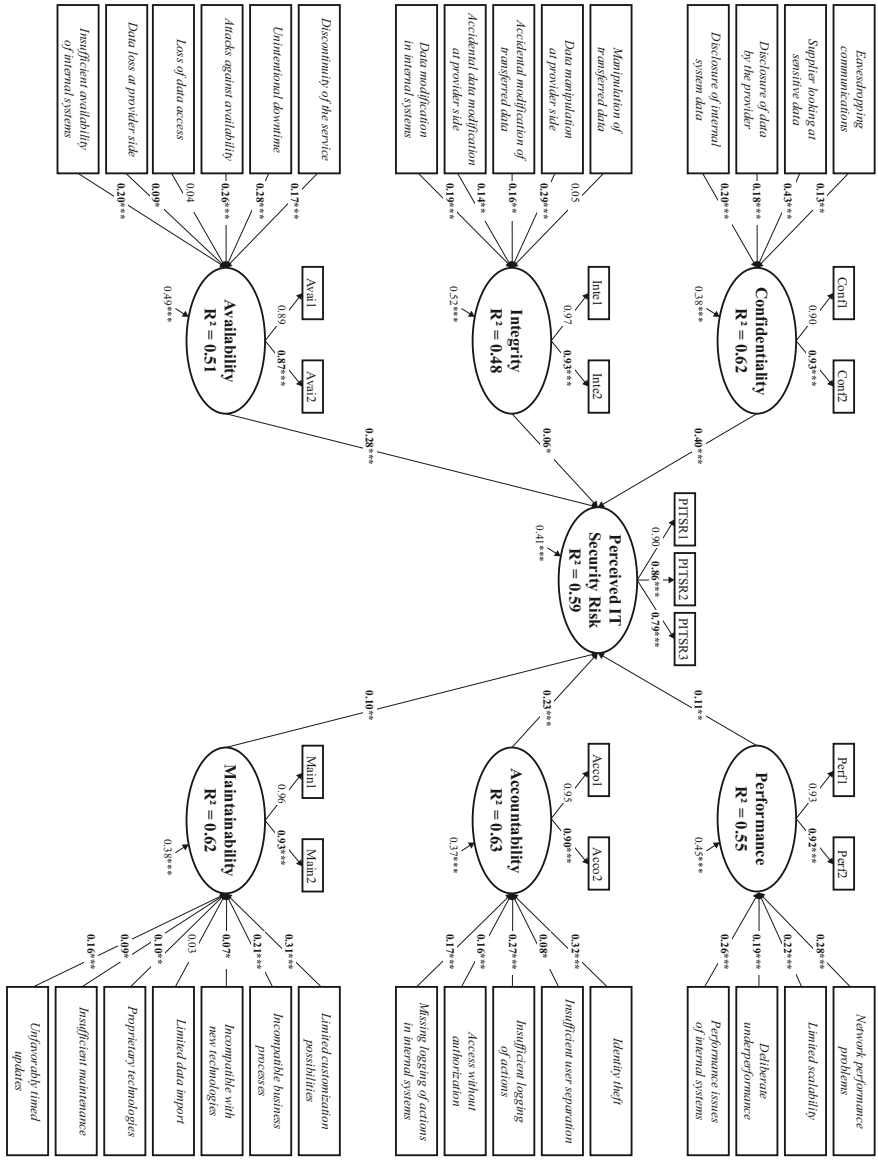


Figure 3.5 Results for the Measurement Model

Table 3.10 Factor Loadings and λ^2 for the Reflective Indicators

Construct	Factor Loadings			λ^2		
Confidentiality	0.898	;	0.931	0.806	;	0.867
Integrity	0.973	;	0.931	0.947	;	0.867
Availability	0.889	;	0.874	0.791	;	0.765
Performance	0.932	;	0.922	0.869	;	0.849
Accountability	0.948	;	0.902	0.900	;	0.813
Maintainability	0.956	;	0.933	0.914	;	0.870
PITSR	0.792	-	0.902	0.627	-	0.813

when the responses are divided into SaaS and IaaS. Therefore, we concluded that all validity characteristics for the set of indicators at the construct level are in an acceptable corridor.

3.5.2.3 Assessing Reliability of the Set of Indicators at the Construct Level

For all reflective indicators, we assessed whether Cronbach's alpha and the Construct Reliability (CR) index by Fornell and Larcker (1981) both exceed the threshold of 0.7 for newly developed measures (Nunnally and Bernstein, 1994). Table 3.9 shows that this is the case for all constructs, which suggests internal consistency reliability of the reflective indicators. The traditional notion of internal consistency reliability does not apply to the formative indicator measurement models of our six first-order risk dimensions, because the causal measurement model does not predict that the indicators will be correlated (MacKenzie et al., 2011, p. 314).

Furthermore, the specified multi-dimensional measurement model does not predict that the sub-dimensions will be correlated and, therefore, reliability does not apply to the set of sub-dimensions serving as formative indicators of PITSR, our focal second-order construct (Edwards, 2001).

3.5.2.4 Evaluating Individual Indicator Validity

The relationships between each reflective indicator and its hypothesized latent construct are large and statistically significant, indicating strong validity of the individual reflective indicators (MacKenzie et al., 2011, p. 314). While the path from each latent variable to its first outcome variable, i. e., the first reflective indicator, has always been fixed to unity (Diamantopoulos, 2011, as recommended by Bollen and

Table 3.11 Significance of Formative Indicators

Construct	Significance ns	*	**	***	Effect on PITSR
Confidentiality	-	-	1	3	***
Integrity	1	-	2	2	*
Availability	1	1	-	4	***
Performance	-	-	-	4	**
Accountability	-	1	-	4	***
Maintainability	1	2	1	3	**

Davis, 2009), all other reflective indicators are highly significant ($p<0.001$). The standardized estimates of the relationships, i. e., the λ parameters, rage from 0.874 to 0.973 for the six risk dimensions, and 0.792 to 0.902 for the indicators of our second-order focal construct PITSR.

We also assessed the degree of validity for each reflective indicator, which is the unique proportion of variance in the indicator accounted for by the construct and which should exceed 0.5. As in our model, all indicators are hypothesized to load on exactly one construct, the degree of validity is equal to square of the completely standardized loading, λ^2 (MacKenzie et al., 2011, p. 314). λ^2 ranges from 0.765 to 0.947 for the six risk dimensions, and reaches 0.627 to 0.813 for our focal construct PITSR. These high values suggest the validity of our selection of reflective indicators.

For first-order latent constructs with formative indicators, we analyzed the paths from indicators to latent construct. All paths are significant, except three indicators that are related to integrity, availability, and maintainability risks. These three formative indicators were therefore considered as candidates for removal in section 3.5.2.6 (MacKenzie et al., 2011, p. 315). The other 28 indicators are significant with $p<0.05$. However, the majority of our formative indicators, i. e., 20 out of 31, have highly significant ($p<0.001$) effects on the constructs.

Second-order latent constructs with first-order sub-dimensions as formative indicators should have sub-dimensions that are significantly related to it. Our six first-order risk dimensions are all significantly related to PITSR with $p<0.05$ (*) for integrity, $p<0.01$ (**) for performance and maintainability, and $p<0.001$ (***) for confidentiality, availability, and accountability. Table 3.11 summarizes the results for formative indicators and the effects of the formative dimensions.

3.5.2.5 Evaluating Individual Indicator Reliability

Regarding to the reliability of the individual indicators, our models passed all tests proposed by MacKenzie et al. (2011, pp. 314–316).

For first-order latent constructs with reflective indicators, we tested whether the squared multiple correlation for each indicator (i. e., the square of the completely standardized loading, λ^2, shown in table 3.10) exceeds 0.5 (Bollen, 1989). The obtained values of 0.765 to 0.947 for the six risk dimensions, and 0.627 to 0.813 for the indicators of our focal construct PITSR suggest that the majority of the variance in the reflective indicators is due to the latent construct.

The reliability of each individual formative indicator was assessed using inter-rater reliabilities during the scale evaluation and refinement steps (MacKenzie et al., 2011, p. 315). All indicators achieved good placement ratios and high Cohen's Kappas during the Q-sort method (see section 3.2), and the interviews with IT security experts showed that almost all experts agreed that the risks are part of their target dimension (see section 3.3).

For PITSR, our focal second-order latent constructs with first-order sub-dimensions as formative indicators, we confirmed that the CR index by Fornell and Larcker (1981) of each dimension as well as the focal construct itself exceeds 0.5. Values of 0.875 to 0.951 for the six risk dimensions, and 0.887 for PITSR support the reliability of each individual sub-dimension.

3.5.2.6 Eliminate Problematic Indicators

According to MacKenzie et al. (2011, p. 316), "problematic indicators are ones that have low validity, low reliability, strong and significant measurement error covariances, and/or non-hypothesized cross-loadings that are strong and significant".

All reflective indicators show highly significant ($p<0.001$) relationships with their latent constructs. The indicator loadings for the first-order risk dimensions are between 0.874 and 0.973, while the three indicators for our focal construct, PITSR, load with 0.792, 0.856, and 0.902.

Conversely, three of our formative indicators have a nonsignificant loading. However, it is important to ensure that all of the essential aspects of the construct domain are captured by the remaining indicators and sub-dimensions when using formative measures (MacKenzie et al., 2011, p. 317). Therefore, in the following, we carefully look at these three indicators and judge whether the exhaustiveness of a dimension would be affected when they are removed.

First, the integrity-related risk that "data are manipulated during transmission" shows a nonsignificant loading and a relatively small path coefficient (0.05). However, all five indicators of the integrity risks dimension (see appendix A.5) clearly

Table 3.12 Construct Variance Inflation Factor

Construct	VIF
Confidentiality	1.678 - 2.358
Integrity	1.861 - 2.549
Availability	1.181 - 1.714
Performance	1.364 - 2.077
Accountability	1.607 - 1.987
Maintainability	1.748 - 2.352

follow the Mutually Exclusive and Collectively Exhaustive (MECE) principle. One measure is related to data modification in internal systems, while the other four are related to external data. These four indicators differ regarding two characteristics: deliberate manipulation vs. accidental modification, as well as data at the provider side vs. data in transit. In order not to violate the collective exhaustiveness, we decided to keep the nonsignificant item related to deliberate manipulation of transferred data. For example, malicious attackers could manipulate the data transferred to the Cloud Computing provider when no or weak encryption is used, e. g., by conducting man-in-the-middle attacks (Dawoud et al., 2010; Jensen et al., 2009).

The second nonsignificant item is the availability-related risk that a company encounters "loss of data access" with a path coefficient of 0.04. The risk could occur because users are no longer able to log on to the service and as a consequence, the service users could end up with no access to their data which are stored on remote servers (Schwarz et al., 2009; Viega, 2009). Despite the nonsignificant loading, we decided to keep this risk as loss of access is an important reason for non-availability in a Cloud Computing context according to the IT security experts interviewed during scale refinement.

Third, the maintainability-related risk that "it is difficult to import existing data into the provisioned application type" shows a relatively small path coefficient (0.03) and a nonsignificant loading. In order to be able to migrate existing data to the new provider, it should be possible (and not too difficult) that data held on existing systems can be used with or incorporated into the new Cloud Computing service. Additionally to limited export functionalities and the related lock-in problem, there is the risk that a provider does not offer adequate possibilities to import existing data (Currie, 2003; Gonçalves and Ballon, 2009). Therefore, we decided to keep this item.

We also tested for redundancy in the indicators using the Variance Inflation Factor (VIF) (see table 3.12). With 1.181 to 2.549, the VIFs for each dimension are always below the cutoff level of 10 (e. g., Diamantopoulos and Winklhofer, 2001),

and the more conservative level of 3 (e. g., Petter et al., 2007). As the three formative indicators cover essential parts of their dimensions, were confirmed by expert interviews, and because analysis of the VIF showed that they are not redundant, we decided to keep them, even if they had insignificant loadings. This is in line with recommendations by Diamantopoulos et al. (2008).

Regarding PITSR as our second-order latent construct with the risk dimensions as its first-order sub-dimensions as formative indicators, all dimensions have a significant loading on PITSR and are therefore unproblematic and no candidates for removal (MacKenzie et al., 2011, p. 317).

3.5.2.7 Assessing Known-Groups Validity of the Construct

Cloud Computing applications can be differentiated into Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS), depending on the type of provided capability (Vaquero et al., 2009). In the following, we compare SaaS, where software applications are provided over the Internet, and IaaS, where processing and storage resources are supplied. In our survey, in total, 250 companies provided values for SaaS-based Cloud Computing, while 104 companies did so for IaaS. PaaS was not tested because of the relatively low sample size.

We first tested whether a dummy variable representing group membership is significantly related to scores on the indicator (MacKenzie et al., 2011, p. 320). Therefore, we measured the correlations of a dummy variable indicating the group membership (SaaS or IaaS) and the formative and reflective indicators. The analysis shows various significant correlations: With a probability of error of less than 10%, 9 out of 31 formative, as well as 4 out of 12 reflective, indicators show significant differences.

Additionally, we performed t-tests for equal mean values in order to analyze whether the average levels of the measures differ across these groups in the hypothesized direction (Cronbach and Meehl, 1955). The results show that there are significant differences between the two groups SaaS and IaaS, especially for maintainability-related risks, where the (mean) reflective indicators differ with a t-statistic of 3.311 and a probability of error of 0.001. The strong significance indicates that maintainability risks, such as limited customization possibilities and proprietary technologies, are perceived to be higher (mean: 4.64) in a SaaS context compared to an IaaS context (mean: 4.14). Table 3.13 shows that for risks related to maintainability, the differences between SaaS and IaaS of 6 out of 7 indicators are strongly significant (with a probability of error of less than 4%). As IaaS is more about basic technology, such as online storage space or processing power on virtual machines, its focus is on hardware, while SaaS is on a higher level of ab-

Table 3.13 Known-Groups Differences

Short Risk Description	Dimension	T-Value	Sign.	SaaS	IaaS
Limited customization possibilities	Maintainability	3.712	0.000	4.68	4.07
Limited data import	Maintainability	3.334	0.001	4.05	3.51
Incompatible with new technologies	Maintainability	2.810	0.005	4.12	3.66
Access without authorization	Accountability	-2.355	0.019	4.16	4.55
Unfavorably timed updates	Maintainability	2.260	0.024	4.26	3.88
Proprietary technologies	Maintainability	2.196	0.029	4.78	4.38
Incompatible business processes	Maintainability	2.103	0.036	4.28	3.91
Network performance problems	Performance	1.952	0.052	4.98	4.66
Insufficient user separation	Accountability	-1.861	0.064	3.93	4.26

straction and has a higher technology stack (Vaquero et al., 2009). Therefore, it is assumed that SaaS is more difficult to integrate into an existing IT landscape and more difficult to maintain compared to IaaS. Another interesting difference (with T: 1.343, p: 0.180) is that performance risks are perceived to be more serious for SaaS (mean: 4,60) compared to IaaS (mean: 4,40). On the contrary, accountability risks are perceived less strong in an SaaS context (mean: 4,75) compared to IaaS (mean: 4,90), with T: -1.102, p: 0.271.

Table 3.13 shows significant differences in t-tests between SaaS and IaaS for selected formative measures where the probability of error was less than 10% with the average values for both groups on a 7-point Likert scale. With a probability of error of less than 10%, 9 out of 31 formative, as well as 3 out of 12 reflective, indicators show significant differences based on the performed T-tests.

Apart from maintainability risks, that are perceived to be more serious in a SaaS context, table 3.13 shows that two accountability-related risks are more dominant when using IaaS: access without authorization and insufficient separation of co-existing users. A possible explanation for the latter could be that the separation of users and resources is mainly an issue at the virtualization layer and therefore nearer to the Cloud Computing infrastructure (Dawoud et al., 2010; Vaquero et al., 2011).

For the two groups SaaS and IaaS, we can attest that there are some indicators and dimensions of IT security risks where the types of Cloud Computing significantly differ. For this reason, the conducted known-groups comparison suggests that the PITSR scale is valid and accurately captures our phenomenon of interest.

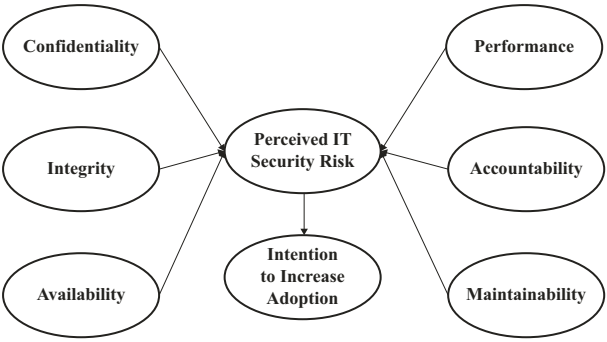


Figure 3.6 Nomological Measurement Model

3.5.2.8 Assessing the Nomological Validity of the Construct

The nomological validity of the PITSR construct was assessed by adding a nomological consequence construct, i. e., the companies' intention to increase their adoption of Cloud Computing. The theoretical consideration of the relationship between perceived risk and adoption have been subject to a number of studies. In line with the Theory of Reasoned Action (Ajzen and Fishbein, 1980), we argue that management's intention to change the level of sourcing based on Cloud Computing depends on its attitude towards Cloud Computing, which is influenced by salient positive and negative beliefs about it. Various studies have confirmed that the intention to increase adoption is directly and negatively related to the perceived risk (e. g., Benlian and Hess, 2011; Gewald et al., 2006; Gewald and Dibbern, 2009). Therefore, we added the company's Intention to Increase Adoption (IIA) to the nomological network as it is caused by PITSR, our focal construct (see figure A.9 in appendix A.8).

According to (MacKenzie et al., 2011, p. 321), the nomological validity of a construct is given, if the estimates of the relationship of PITSR and its hypothesized consequence IIA are significant and show the anticipated sign. The highly significant, negative path coefficient between PITSR and IIA (β=-0.53, $p<0.001$), and the ratio of explained variance of IIA (R^2 =0.28) strongly confirm the hypothesized relationship. This result is consistent with prior theory and shows that the indicators of our focal construct relate to measures of other constructs in the manner expected. Hence, we can conclude that our measure of perceived IT security risk related to Cloud Computing is nomologically valid.

The strong relation between the perceived IT security risk and the intention to increase adoption is an important theoretical contribution to the IT security and IT risk literature. Although it has been shown that there are many factors influenc-

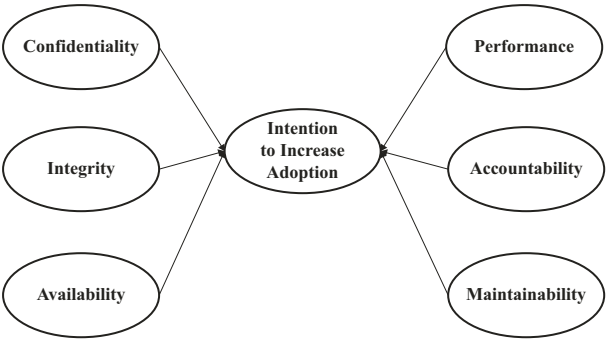


Figure 3.7 Nomological Measurement Model with First-Order Constructs Only

ing the adoption decision of potential customers, such as subjective norm (Fishbein and Ajzen, 1975), perceived benefits (Chwelos et al., 2001) and opportunities (Gewald and Dibbern, 2009), as well as other types of risks, e. g., economic and strategic risk (Benlian and Hess, 2011), the perceived IT security risk alone explains 28% of the intention's variance. Therefore, future research regarding the Cloud Computing decision process should incorporate PITSR as one of the major influencing factors.

3.5.2.9 Using the Nomological Network to Assess the Validity of the Multi-Dimensional Structure

Regarding the nomological network, we also performed the tests described by MacKenzie et al. (2011, pp. 322f.) in order to evaluate the adequacy of the multi-dimensional structure of the PITSR construct. As we deal with a formatively measured, second-order focal construct and a nomological consequence construct (IIA), the hypothesized structure was assessed by testing whether the sub-dimensions have insignificant or weak direct effects on the consequence construct.

Our tests show that confidentiality, integrity, and maintainability do not have significant effects (with $p<0.05$) on IIA, indicating that the multi-dimensional structure for these dimensions is consistent with the data. The other three dimensions have significant direct effects on IIA, but all these effects are weaker than the direct effect of the focal construct on the consequence. Therefore, there is enough evidence to support the adequacy of the hypothesized multi-dimensional structure.

Additionally, we performed comparisons proposed by Stewart and Segars (2002) (also used by Bansal, 2011) in order to assess the validity of the multi-dimensional structure. Therefore, we compared the nomological network shown

Table 3.14 Validity of the Multi-Dimensional Structure

Statistic	Second-order Construct (See Figure 3.6)	First-order Constructs Only (See Figure 3.7)
N	354	354
chi^2	1,600	1,331
df	655	518
chi^2/df	2.443	2.569
GFI	0.834	0.847
RMSEA	0.068	0.072
SRMR	0.075	0.069
CFI	0.982	0.981
NFI	0.970	0.970
TLI	0.967	0.963

in figure 3.6 to a nomological network without the focal, second-order construct, i. e., all dimensions are directly linked to the IIA (see figure 3.7).

Comparison of the goodness of fit indices shows that the multi-dimensional model which includes the focal construct exhibits a lower chi^2/df ratio as well as slightly better RMSEA, CFI, and TLI. These results also suggest that PITSR may be represented as a second-order factor structure rather than a set of six first-order factors.

The validated multi-dimensional structure of perceived IT security risk related to Cloud Computing is an important contribution of this thesis. While previous studies treated security related risks as simple, one-dimensional measures (e. g., Chellappa and Pavlou, 2002; Flavián and Guinalíu, 2006; Casalo et al., 2007; Kim et al., 2008; Pavlou et al., 2007), they did not fully represent the construct's complex structure. The developed dimensions of IT security risks are based on the structured literature review, and have been successfully validated using the Q-sort method, expert interviews, and nomological tests using the responses of the conducted quantitative study.

Table 3.15 Inter-Constuct Discriminant Validity

Construct	$\sqrt{\text{AVE}}$	Max. Inter-Construct Correlation
Confidentiality	0.915	0.614
Integrity	0.952	0.385
Availability	0.881	0.515
Performance	0.926	0.326
Accountability	0.925	0.505
Maintainability	0.944	0.333
PITSR	0.851	0.614

3.5.2.10 Assess Discriminant Validity

Discriminant validity can be assessed regarding two aspects: First, we tested the inter-construct discriminant validity for all constructs used in the model. Therefore, we assessed whether the measurements of different constructs are significantly different from each other. We used the test proposed by Fornell and Larcker (1981, p. 46) which compares the Average Variance Extracted (AVE) of a construct to the squared correlations between the construct and any other construct. As the squared correlation between two constructs can be interpreted as their shared variance, discriminant validity is given, if this shared variance is smaller than the AVE of the constructs (Weiber and Mühlhaus, 2009, p. 135). Table 3.15 reports the square root of the AVE for each dimension and for the focal construct PITSR as well as the maximum inter-construct correlation.

Second, additionally to validating that our indicators provide an accurate representation of the perceived IT security risk related to Cloud Computing and that they behave in a manner that is consistent with the nomological network, we also tested whether our indicators are distinguishable from already existing indicators of other constructs. Therefore, we included the construct of "Perceived Negative Utility" (also called perceived risks or costs) with measures adapted from Benlian and Hess (2011) as well as Featherman and Pavlou (2003) in our study. The construct will be introduced in more detail in section 3.6.

As the perceived IT security risk is a facet of the overall perceived negative utility of using Cloud Computing (next to, e. g., perceived financial and strategic risks), we tested whether the proposed PITSR scale (without the nomological IIA construct) is distinguishable from the construct "Perceived Negative Utility". The construct intercorrelation between both constructs is 0.423, which is far below the threshold of 0.71 given by MacKenzie et al. (2011, p. 324). This means that there is

sufficient evidence that the discriminant validity of the PITSR scale to the overall perceived risk scale is acceptable.

As our constructs were also measured using reflective indicators, we also successfully tested that the AVE for the two constructs (0.674 for PITSR and 0.574 for Perceived Negative Utility) are both greater than the square of the correlation ($0.423^2 = 0.179$). This result also indicates that the two similar constructs are distinct (Fornell and Larcker, 1981, p. 46).

3.6 Analysis of Adoption Decisions

One of the key questions, this thesis addresses, is how IT executives perceive the IT security risks of Cloud Computing and which risks influence their adoption decisions related to this paradigm. Therefore, we included additional questions in the questionnaire asking for the behavioral intention to increase the level of Cloud Computing adoption and the related negative and positive attitudes towards the adoption. Based on these questions, in this section, we analyze whether IT executives' perception of risks and opportunities affects the level of Cloud Computing adoption.

In more detail, this section assesses which specific risks are most influential in forming firms' adoption decisions. Therefore, a Structural Equation Model (SEM) is build to analyze the effect of risks and opportunities on the adoption intention based on the in-depth conceptualization of Perceived IT Security Risk (PITSR) and the developed measurement scale.

3.6.1 Theoretical Perspective and Hypothesis Development

In this section, we develop the theoretical rationale for our research model shown in figure 3.8. We first present the hypotheses related to the impact of positive and negative attitudinal appraisals of Cloud Computing adoption on behavioral intentions, followed by hypotheses related to the dual impact of perceived IT security risks on these positive and negative attitudinal concepts.

In line with the construct conceptualization and formal measurement specification (see section 3.4.1), we model the aggregated perceived IT security risk as a multi-dimensional construct. According to the decision rules given by Jarvis et al. (2003, p. 203), we build a formative first-order, formative second-order model for the perceived IT security risk related to Cloud Computing. We, therefore, model a causal relationship between the identified individual risk items and the six risk dimensions. Additionally, all sub-dimensions are formative indicators of the aggregated perceived IT security risk construct.

Consistent with previous studies on risk perception that already included subscales and multiple risk dimensions (Peter and Tarpey, 1975; Havlena and DeSarbo, 1990; Mitchell and Greatorex, 1993; Featherman et al., 2006; Benlian and Hess, 2011), we derive the first six hypothesis. All IT security risk dimensions have been identified during development of measures using a literature review (see section 3.1) and have been successfully evaluated using the Q-sort method (see section 3.2) and expert interviews (see section 3.3). For each dimension, the

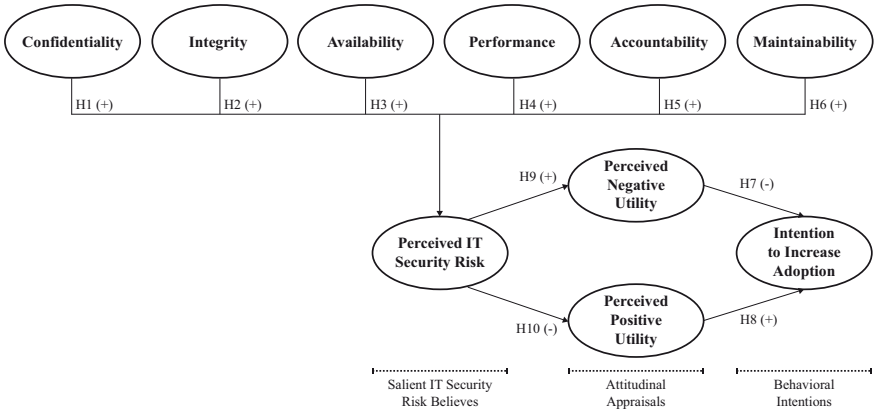


Figure 3.8 Adoption Decisions Measurement Model

IT executives' beliefs regarding the perceived risk related to the dimension (e. g., confidentiality or availability) are positively related to the aggregated perceived IT security risk. This means that if the risk in the dimension is perceived to be stronger, then the aggregated perceived IT security risk construct's score should also reflect this increased risk. The following hypotheses were all already tested during scale assessment and validation in section 3.5.2:

Hypothesis 1. IT executives' beliefs regarding *confidentiality* risks of Cloud Computing are positively related to the aggregated perceived IT security risk.

Hypothesis 2. IT executives' beliefs regarding *integrity* risks of Cloud Computing are positively related to the aggregated perceived IT security risk.

Hypothesis 3. IT executives' beliefs regarding *availability* risks of Cloud Computing are positively related to the aggregated perceived IT security risk.

Hypothesis 4. IT executives' beliefs regarding *performance* risks of Cloud Computing are positively related to the aggregated perceived IT security risk.

Hypothesis 5. IT executives' beliefs regarding *accountability* risks of Cloud Computing are positively related to the aggregated perceived IT security risk.

Hypothesis 6. IT executives' beliefs regarding *maintainability* risks of Cloud Computing are positively related to the aggregated perceived IT security risk.

Numerous studies in the field of IS have found that adoption decisions related to ITO are major management decisions that are made by an organization's top IT executive (Apte et al., 1997). For example, previous research has found that the decision to outsource IT is primarily driven and controlled by either the top management (i. e., CEO) or IT management (i. e., CIO) (Willcocks et al., 1996;

Hirschheim and Lacity, 2000). Thus, the ITO decision process is related to IT executives, i. e., individual entities rather than whole organizations. In order to model the decision-making process of these individuals, conceptual (stage) models have been developed that represent senior managers' cognitive evaluation processes of sourcing options and the resulting outcomes (Simon, 1960; Dibbern, 2004). Based on the risk-benefit concept of decision theory (Machina, 1987; Howard, 1988; Valacich et al., 2009), in the first stage of these models, decision makers assess the advantages and disadvantages of an ITO adoption decision by weighing their perceived positive and negative utility. The concept assumes that actions are reasoned by balancing risks against opportunities, i. e., mental representations and evaluations of possible future outcomes. Thereby, the models explicitly embody cognitive processes related to establishing intentions that form ITO adoption decisions (Ajzen and Fishbein, 1980; Smith, 1992).

The Theory of Reasoned Action (TRA), an intention model suggesting that the decision to engage in a specified behavior is determined by an individual's intention to perform this behavior, has been widely investigated. The theory suggests that the behavioral intention to act is formed by, both, the attitude toward the behavior and the so-called subjective norm, i. e., normative beliefs as well as the motivation to comply with these beliefs (Fishbein and Ajzen, 1975; Ajzen and Fishbein, 1980). Studies using the TRA in IT adoption- and IT outsourcing-related contexts indicated that attitudes of IT executives are generally accurate predictors of their individual future behavioral intentions (e. g., Harrison et al., 1997). As the TRA suggests an active and deliberate decision process, it provides a useful and appropriate theoretical lens for our analysis regarding IT executives' mental assessments of the positive and negative utility of Cloud Computing adoption. Accordingly, the theory can be used in order to explain how IT security risks affect the trade-off between positive and negative utility.

Comparable to Benlian and Hess (2011, p. 235), we draw on the TRA's main line of reasoning, i. e., we focus on how IT executives' attitude towards Cloud Computing adoption are formed by salient behavioral beliefs and neglect the effect of the subjective norm (and normative beliefs). Consequently, we analyze the belief-attitude-intention relationship (see figure 3.8) and argue that IT executives' intention to adopt Cloud Computing services is affected by their positive and negative attitudinal appraisals of Cloud Computing adoption, which are in turn influenced by salient IT security risk beliefs about Cloud Computing. More specifically, we hypothesize that perceived IT security risk (consisting of the six identified distinct security dimensions) is a salient antecedent that affects positive as well as negative attitudes that subsequently influence behavioral adoption intentions and actions. Therefore, we argue that IT executives assess different IT security related risks that may arise from Cloud Computing adoption, combine these assessments

into both positive and negative attitudinal appraisals that collectively influence IT executives' Cloud Computing adoption intentions.

Applying the TRA to the Cloud Computing adoption context, we hypothesize that Cloud Computing adoption intentions are determined by IT executives' overall attitudinal appraisal of the negative and positive utility associated with Cloud Computing adoption. This is in line with previous studies that showed that the perceived negative utility (also called perceived risks or costs) influences IT adoption processes. For example, Featherman and Pavlou (2003) and Kim et al. (2008) found that perceived risk significantly affected the intention of individual consumers to increase their level of Internet-based services and applications such as, e. g., bill payment services. Likewise, Gewald et al. (2006) and Gewald and Dibbern (2009) showed that perceived risk has a negative effect on IT managers' intention to adopt Business Process Outsourcing (BPO).

In addition to this, empirical studies showed that the IT executives' perceived positive utility (also called perceived opportunities or benefits) of IT adoption affect their intention to increase the level of adoption of ITO and BPO. An empirical study showed that adoption decisions of IT managers in the German banking industry were strongly affected by their perceived opportunities in BPO (Gewald and Dibbern, 2009). Similarly, Chwelos et al. (2001) found a significant effect of the perceived benefits of Electronic Data Interchange (EDI) on IT executives' EDI adoption intentions. Based on the described theoretical foundations and empirical findings, we expect that IT executives' attitudinal appraisals of the positive and negative utility of Cloud Computing adoption have a significant role in forming Cloud Computing adoption intentions. Consequently, we hypothesize that:

Hypothesis 7. IT executives' perceptions of the negative utility of Cloud Computing adoption are negatively related to their intention to increase the level of Cloud Computing adoption.

Hypothesis 8. IT executives' perceptions of the positive utility of Cloud Computing adoption are positively related to their intention to increase the level of Cloud Computing adoption.

Our following hypothesis on IT security risk's influence on the overall perceived negative utility (i. e., overall perceived risk) of Cloud Computing adoption is based on Cunningham's (1967) perceived risk framework. As already described in section 2.2.2, in adoption-related contexts, perceived negative utility is often explained as "the felt uncertainty regarding the possible negative consequences of adopting a product or service" (Benlian and Hess, 2011). Peter and Ryan (1976, p. 185) define the concept as the "expectation of losses associated with purchase" and emphasize its inhibitory role related to purchase behavior. Accordingly, the concept of perceived negative utility can be applied in adoption situations in which a decision maker is uncertain and uncomfortable, or that create anxiety (Bettman,

1973). Drawing on these definitions, we define perceived negative utility of Cloud Computing adoption as the potential for loss in the pursuit of a desired outcome when adopting Cloud Computing services.

Featherman and Pavlou (2003, pp. 454f.) typifies the overall perceived risk as having five dimensions that are related to (1) performance, (2) financial, (3) time, (4) psychological/social, and (5) privacy. A considerable amount of literature in the field of individual and organizational behavior has been published on the dimensions of perceived risk and how risk influences product and service evaluations (e. g., Featherman and Pavlou, 2003; Kim et al., 2008). Adopting this framework to the IT outsourcing and Cloud Computing context, several studies found that IT security risk is one of, if not the most prevalent factor affecting overall perceptions of risks associated with IT adoption and outsourcing decisions. For example, Benlian and Hess (2011) showed in an empirical study of SaaS adopters and non-adopters that IT security risks had the greatest impact on negative attitudinal evaluations of SaaS adoption. Gewald and Dibbern (2005) found that performance and privacy risks significantly affected companies' overall perceived risk related to the acceptance of business process outsourcing in the German banking industry.

Whenever Cloud Computing is used as a sourcing model, clients face a multitude of risks (see section 3.4.2 for descriptions of the IT security-related risks identified during the development of measures). As the development of Internet-based technologies is highly dynamic, Cloud Computing is subject to environmental uncertainties. Thus, IT executives may feel anxiety and discomfort because of this unpredictability. Assuming that decision makers anticipate possible IT security risks, we hypothesize that perceived IT security risks form an important salient belief that increases IT executives' feelings of uncertainty (i. e., perceptions of negative utility) of Cloud Computing adoption:

Hypothesis 9. IT executives' perceptions of Cloud Computing adoption's IT security risks are positively related to their attitudinal appraisals of the negative utility of Cloud Computing adoption.

At the same time, we argue that IT security risk will also have an adverse effect on overall positive attitudinal appraisals (i. e., perceived positive utility) of Cloud Computing adoption. Previous literature suggested that Cloud Computing brings about major operational improvements through cost reduction and standardization opportunities as well as strategic flexibility (Armbrust et al., 2010; Cusumano, 2010). Cost advantages arise because external vendors can provide IT functions, such as application services, at lower costs than client companies can. Since Cloud Computing is based on the principles of virtualization and multi-tenancy, providers can realize supply-side economies of scale because a single server is able to serve multiple clients in parallel (Buxmann et al., 2011a, p. 11). This improved economics in the provision of Cloud Computing-based services (compared to tradi-

tional, isolated software and hardware installations) can be passed on to the clients, who may benefit from the provider's cost-efficient architecture by having lower total costs of ownership. Due to the on-demand self service and the rapid elasticity (see section 2.1), Cloud Computing customers may experience a higher strategic flexibility because the large operational investments that have to be paid in advance are shifted to the provider (Lacity et al., 1995, 2010). Therefore, Cloud Computing potentially reduces the vendor lock-in effects arising because of high switching costs that are a common characteristic of traditional on-premises software and hardware installations (Buxmann et al., 2008, p. 501).

When clients perceive strong potential IT security risks, however, their overall assessment of Cloud Computing services' benefits may suffer. Cost advantages through using Cloud Computing may disappear because of precautions that have to be taken against IT security threats. Moreover, potential benefits due to higher strategic flexibility in switching Cloud Computing providers may be foregone, since (relationship-) specific investments in establishing and ensuring IT security may increase transaction costs again (Whitten and Wakefield, 2006, p. 230). Previous research studies in e-services adoption have also found that different perceived risk facets decrease the perceived usefulness of e-services adoption and subsequently reduce adoption intentions (Featherman and Pavlou, 2003; Featherman and Wells, 2010). Thus, we hypothesize as follows:

Hypothesis 10. IT executives' perceptions of Cloud Computing adoption's IT security risks are negatively related to their attitudinal appraisals of the positive utility of Cloud Computing adoption.

Taken together, we argue that perceived IT security risk assumes a dual role in affecting IT executives' Cloud Computing adoption intentions. It not only nurtures IT executives' uncertainties and feelings of negative utility of Cloud Computing adoption, but also attenuates IT executives' positive attitudinal appraisals by diminishing Cloud Computing adoption's overall usefulness (i. e., perceptions of positive utility). Figure 3.8 visualizes the final opportunity-risk model of Cloud Computing adoption decisions and the ten related hypotheses that have been developed.

3.6.2 Description of Measures

In addition to the model shown in figure 3.5 with its risk dimensions and items formally specified in section 3.4.1 and described in detail in section 3.4.2, we included the nomological construct Intention to Increase Adoption (IIA) in order to

Table 3.16 Additional Questionnaire Items for the Adoption Model

Constructs	Indicators
	To what extent do you agree with the following statements?
Perceived Negative Utility (PNU)	• Adopting Cloud Computing is associated with a high level of risk. • There is a high level of risk that the expected benefits of adopting Cloud Computing will not materialize. • Overall, I consider the adoption of Cloud Computing to be risky. Source: Indicators are based on Featherman and Pavlou (2003)
Perceived Positive Utility (PPU)	• Adopting Cloud Computing has many advantages. • Adopting Cloud Computing is a useful instrument for increasing operational excellence. • Overall, I consider the adoption of Cloud Computing to be a useful strategic option. Source: Indicators are based on Gewald and Dibbern (2009)
Intention to Increase Adoption (IIA)	• If there is a superior offer, Cloud Computing should be used for the application domain I am in charge of. • Our company should increase the existing level of adopting Cloud Computing. • I support the further adoption of Cloud Computing. Sources: Indicators are based on Gewald and Dibbern (2009); Benlian and Hess (2011)

measure the behavioral intention to increase the level of Cloud Computing adoption. The IIA construct was also used for tests regarding the nomological validity and the validity of the multi-dimensional structure in sections 3.5.2.8 and 3.5.2.9.

Furthermore, we added two new constructs related to the Perceived Negative Utility (PNU) as well as the Perceived Positive Utility (PPU). Table 3.16 provides our conceptual definition of these additional constructs and a summary of the sources from which the items for the scales were drawn. Content and face validity were established by adopting validated measurement items from previous research studies with minor changes in wording. The indicators for these two constructs are based on Featherman and Pavlou (2003) and Gewald and Dibbern (2009). All nine indicators were measured using a seven-point Likert scale, with 1 referring to the lowest score (i. e., complete disagreement) and 7 to the highest score (i. e., complete agreement) on the item scale.

Table 3.17 Goodness of Fit of the Adoption Decisions Measurement Model

Statistic	Adoption Model
N	354
chi^2	2,133
df	955
chi^2/df	2.233
GFI	0.814
RMSEA	0.061
SRMR	0.080
CFI	0.980
NFI	0.965
TLI	0.969

3.6.3 Results of the Statistical Analysis

The result data set obtained from our empirical survey (see section 3.5.1) was used to calculate all statistics for the presented models. In our data analysis, we tested our research hypotheses using Covariance Structure Analysis (CSA)-based structural equation modeling. In order to obtain results comparable to those of section 3.5, we employed LISREL (version 8.80; Jöreskog and Sörbom, 2006). As we wanted to analyze how well all indicators together explain each construct and in order to be able to assess the disturbance terms, CSA was used instead of Partial Least Squares (PLS), which is said to provide less accurate parameter estimations (Gefen et al., 2003, p. 68). The results are shown in tables 3.17 and 3.18.

The calculated goodness of fit statistics are comparable to those obtained for the developed scale in section 3.5.2.1 (see table 3.8). With its 955 degrees of freedom (df), the model has a chi^2 statistic of 2,133. The chi^2/df ratio of 2.233 indicates a good model fit (Carmines and McIver, 1981; Wheaton et al., 1977). Regarding the absolute fit of the model, measured by SRMR, GFI, and RMSEA, we received mixed results. As the model is even more complex that the one used during scale development (see figure 3.5), the results of the relative fit indices, which are less sensitive to sample size, should be considered (Hu and Bentler, 1999; Hilkert et al., 2011). The CFI of 0.980 indicates a good model fit. Likewise, the NFI of 0.965 as well as the TLI, also called NNFI, of 0.969 are all above the threshold of 0.95 proposed by Hu and Bentler (1999, p. 27). For these reasons, we concluded that our adoption-related measurement model has an acceptable goodness of fit.

Table 3.18 Factor Loadings, AVE, and CR for the Adoption Decisions Measurement Model

Construct	Factor Loadings			AVE	CR
Confidentiality	0.898	;	0.931	0.837	0.911
Integrity	0.973	;	0.931	0.907	0.951
Availability	0.885	;	0.880	0.779	0.876
Performance	0.932	;	0.922	0.859	0.924
Accountability	0.949	;	0.901	0.856	0.922
Maintainability	0.956	;	0.932	0.891	0.943
PITSR	0.781	-	0.900	0.719	0.884
PNU	0.469	-	0.915	0.558	0.780
PPU	0.638	-	0.864	0.550	0.783
IIA	0.827	-	0.893	0.752	0.901

All completely standardized factor loadings for the new constructs are significant, thus suggesting convergent validity. Additionally, all constructs also meet the recommended threshold value for the Average Variance Extracted (AVE) (i. e., AVE > 0.5). The AVE ranges from 0.779 to 0.907 for the six security risk dimensions, and takes values of 0.719 for the perceived IT security risk, 0.558 and 0.550 for PNU and PPU, and 0.752 for the intention to increase the Cloud Computing adoption.

To evaluate construct reliability, we calculated the Construct Reliability (CR) of each construct. All constructs have a CR level that is significantly above the recommended cutoff value of 0.7 (Fornell and Larcker, 1981; Nunnally and Bernstein, 1994). Table 3.18 shows that the CR-values for the adoption decisions measurement model range from 0.780 to 0.951, indicating internal consistency and reliability of the indicators.

The validity of the individual indicators was assessed by testing for large and statistically significant relationships between each indicator and its hypothesized latent construct. The completely standardized factor loadings, i. e., the λ parameters, range from 0.880 to 0.973 for the six dimensions of security risks, 0.781 to 0.900 for the perceived IT security risk, 0.469 to 0.915 for the perceived negative utility, 0.638 to 0.864 for the perceived positive utility, and 0.827 to 0.880 for the intention to increase the level of Cloud Computing adoption (see table 3.18).

Regarding the discriminant validity of the latent variables, the loadings of our reflective indicators are higher with regard to their respective constructs than with regard to any other construct.

Additionally, for all except one construct (i. e., PPU), the square roots of the AVEs exceed the inter-construct correlations between the independent constructs,

which are relatively low. The AVE of the perceived positive utility is 0.55, while its inter-construct correlation with IIA is 0.829 ($\sqrt{0.55} \approx 0.742 < 0.829$). In case of all other constructs, the latent variables' discriminant validity is supported (Fornell and Larcker, 1981, p. 46; Weiber and Mühlhaus, 2009, p. 135).

The results in figure 3.9 indicate that 61% of the variance in perceived IT security risk involved in the use of Cloud Computing are explained by its constituting facets. Surprisingly, 47% of the variance in the perceived negative utility are explained solely by the perceived IT security risk. In addition, 25% of the variance in perceived positive utility are explained. Finally, perceived positive and negative utility together explain 74% of the variance in intention to increase the level of Cloud Computing adoption. The results also show that the path coefficients in the research model are all significant. Overall, the data supported all our ten hypotheses.

Hypotheses 1–6. As already shown during scale development in section 3.5.2, the perceived risks in each sub-dimension positively and significantly affect PITSR. Thus, hypotheses 1 to 6 are supported. While integrity risks are related with a relatively low β of 0.05 (with $p<0.05$, i. e., *), risks related to maintainability and performance show higher β path coefficients of 0.09 and 0.13 with $p<0.01$ (**). The other three security risk dimensions, i. e., accountability, availability, and confidentiality, are highly significant with $p<0.001$ (***) and completely standardized path coefficients of 0.20, 0.29, and 0.42.

This means that the perceived IT security risk is largely affected by confidentiality-related risks, such as the supplier looking at sensitive data (e. g., Beulen et al., 2005; Briscoe and Marinos, 2009; Schwarz et al., 2009), attackers eavesdropping communications (e. g., Jensen et al., 2009; Viega, 2009; Dawoud et al., 2010), or that data are disclosed by the provider (e. g., Itani et al., 2009; Kaufman, 2009; Viega, 2009).

Hypothesis 7. The first effect which we hypothesized to be negative was the effect of IT executives' overall perceived negative utility of Cloud Computing on their intention to increase the level of Cloud Computing adoption. The results shown in figure 3.9 support hypothesis 7. The relation is highly significant with $p<0.001$ (i. e., ***) and has a moderate path coefficient β=-0.24.

Hypothesis 8. The highest measured, very large path coefficient of β=0.75 indicates very strong support for hypothesis 8, that the IT executives' overall perceived positive utility of Cloud Computing are positively related to their intention to increase the level of Cloud Computing adoption. The relation is highly significant (i. e., ***) with $p<0.001$.

Our results show that perceived positive and negative utilities were not factored into adoption decisions to the same extend. With a path coefficient of 0.75, the perceived positive utility seems to have a much stronger effect on the adoption

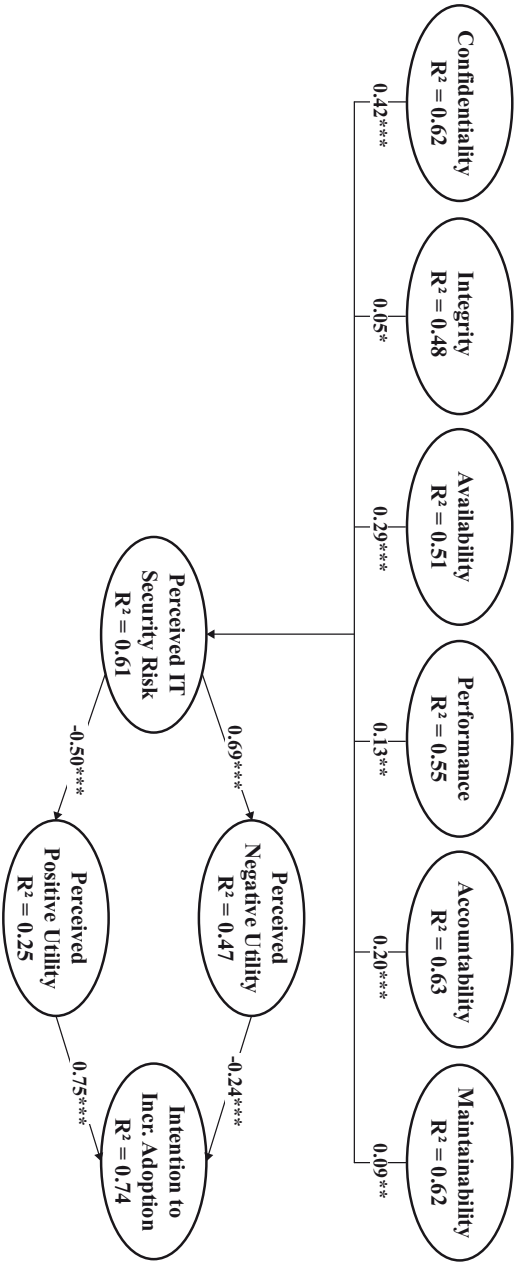


Figure 3.9 Results for the Adoption Decisions Measurement Model

intention than the perceived negative utility has (with a path coefficient of -0.24). This stronger effect of benefits or opportunities was already found in previous adoption-related studies (Gewald and Dibbern, 2005, 2009; Benlian and Hess, 2011).

Hypothesis 9. Furthermore, the data indicates that the IT executives' beliefs regarding IT security risks of Cloud Computing are positively related (β=0.69, $p<0.001$, i. e., ***) to the overall perceived negative utility. This is in line with previous studies that found that IT security related risks are one of, it not the major risk factor affecting outsourcing and adoption decisions (e. g., Gewald and Dibbern, 2005; Benlian and Hess, 2011).

Hypothesis 10. Finally, the perceived IT security risk shows a highly significant negative effect on the overall perceived positive attitudes towards Cloud Computing adoption (β=-0.50, $p<0.001$, i. e., ***). This is an important contribution as our hypothesized model is a departure from previous research on perceived risk where IT security risk just had an effect on negative utility assessments (e. g., Benlian and Hess, 2010, 2011). Thus, this thesis provides a more nuanced view of the nature and dual inhibitory role of perceived IT security risks in Cloud Computing adoption decision-making processes.

In order to assess the effect of perceived IT security risks on the intention to increase the level of Cloud Computing adoption, the total effects of PITSR on IIA can be used. These effects indicate, how much a one unit change in one construct will change the expected value of another construct. As PITSR was modeled not to have any direct effects on IIA (see figure 3.9), the total effects are equal to the indirect effects. These represent the influence of one construct on another as mediated by one or more intervening variables (Diamantopoulos and Siguaw, 2000, pp. 69f.), i. e., the overall perceived negative and positive utility in our model.

Our LISREL-based data analysis shows that the perceived IT security risk related to Cloud Computing has standardized total effects of -0.540 on the IT executives' intention to increase the level of adoption. The highly significant t-value of -10.312, i. e., ***, indicates that, with a probability of error of less than one per mil, PITSR has an effect on IIA.

Table 3.19 shows the standardized total effects of each security risk dimension on the intention to increase the level of Cloud Computing adoption. The effects of the confidentiality-, availability-, and accountability-related risks are highly significant (i. e., ***) and negative. In particular, the security risk dimension "confidentiality" shows strong indirect effects on IIA, where a one unit change in the confidentiality construct will reduce the expected value of the IIA construct by more than 0.2.

Table 3.19 Total Effects of Risk Dimensions on Adoption Intentions

Construct	Total Effects on IIA	T-Value
Confidentiality	-0.226	-6.930
Integrity	-0.025	-1.013
Availability	-0.157	-5.428
Performance	-0.070	-2.845
Accountability	-0.107	-4.040
Maintainability	-0.049	-2.054

Performance (**) and maintainability (*) also show significant negative effects on the intention to increase the level of adoption, but these effects are less strong than for the already mentioned security risk dimensions.

The least strong total effect is related to integrity risks, where the t-value of -1.013 indicates that the effect is significant with a probability of error of more than 5%.

The standardized total effects of each individual security risk item on the adoption intention are shown in table 3.20. The table is sorted in decreasing order of the effect on IIA which means that the risks with the strongest impact are at the top of the table.

Six IT security risks of the top seven listed risks show highly significant (i. e., ***) total effects: “Supplier looking at sensitive data” (e. g., Beulen et al., 2005; Briscoe and Marinos, 2009; Schwarz et al., 2009), “Unintentional downtime” (e. g., Aron et al., 2005; Benefield, 2009; Yildiz et al., 2009), “Disclosure of internal system data”, “Attacks against availability” (e. g., Bhattacharya et al., 2003; Jensen et al., 2009; Zhang et al., 2009), “Identity theft” (e. g., Goodman and Ramer, 2007; Jensen et al., 2009; Viega, 2009), and “Insufficient availability of internal systems”.

Out of these risks, three are related to the availability (of services and internal systems). The other three highly significant risks consist of two confidentiality- and one accountability-related risks.

Another confidentiality risk is ranked fifth based on its total effect (-0.041), but its relatively smaller t-value of -3.043 (**, i. e., $p<0.01$) suggests that the effect is less significant than the former seven risks: The risk that data fall into the wrong hands because of (intentional or accidental) disclosure by the provider (e. g., Itani et al., 2009; Kaufman, 2009; Viega, 2009) seems to be another very important risk for the (potential) users of Cloud Computing.

It should be noted that two of the significant top seven risks are related to internal systems and data. Both security risk items were not found during the liter-

Table 3.20 Strongest Total Effects of Individual Risks on Adoption Intentions

Short Risk Description	Dimension	Total Effects on IIA	T-Value
Supplier looking at sensitive data	Confidentiality	-0.096	-5.202
Unintentional downtime	Availability	-0.045	-3.871
Disclosure of internal system data	Confidentiality	-0.044	-3.588
Attacks against availability	Availability	-0.041	-3.817
Disclosure of data by the provider	Confidentiality	-0.041	-3.043
Identity theft	Accountability	-0.034	-3.524
Insufficient availability of internal systems	Availability	-0.031	-3.424
Insufficient logging of actions	Accountability	-0.029	-3.286
Eavesdropping communications	Confidentiality	-0.029	-2.497
Discontinuity of the service	Availability	-0.026	-2.853
Network performance problems	Performance	-0.019	-2.527
Missing logging of actions in internal systems	Accountability	-0.018	-2.587
Performance issues of internal systems	Performance	-0.018	-2.563
Access without authorization	Accountability	-0.017	-2.468
Limited customization possibilities	Maintainability	-0.016	-1.946
Limited scalability	Performance	-0.015	-2.296
Data loss at provider side	Availability	-0.014	-1.635
Deliberate underperformance	Performance	-0.013	-2.256
Incompatible business processes	Maintainability	-0.010	-1.812
Insufficient user separation	Accountability	-0.009	-1.585
Unfavorably timed updates	Maintainability	-0.008	-1.720
Data manipulation at provider side	Integrity	-0.007	-0.991
Proprietary technologies	Maintainability	-0.005	-1.427
Data modification in internal systems	Integrity	-0.005	-0.976
Loss of data access	Availability	-0.005	-0.578
Insufficient maintenance	Maintainability	-0.004	-1.273
Incompatible with new technologies	Maintainability	-0.004	-1.188
Accidental modification of transferred data	Integrity	-0.004	-0.943
Accidental data modification at provider side	Integrity	-0.004	-0.930
Limited data import	Maintainability	-0.002	-0.650
Manipulation of transferred data	Integrity	-0.001	-0.559

ature review (see section 3.1) and were added during the expert interviews (see section 3.3). This is an indication that the comprehensive conceptualization contributes to the existing literature, which seems to be lacking some of the security risks that mostly affect the IT executives' intention to increase the level of Cloud Computing adoption.

3.6.4 Discussion of the Survey's Results

As a result of chapter 3, it has been shown that our proposed multi-dimensional conceptualization of perceived IT security risk related to Cloud Computing is more suitable than the measures used in previous studies which relied on simple, unidimensional and/or inconsistent conceptualizations (e. g., Chellappa and Pavlou, 2002; Flavián and Guinalíu, 2006; Casalo et al., 2007; Kim et al., 2008; Pavlou et al., 2007). The developed scale was successfully evaluated and the results provide evidence for the validity of the multi-dimensional structure.

Table 3.21 The Ten Highest Rated IT Security Risks of Cloud Computing

Short Risk Description	Dimension	Mean
Identity theft	Accountability	5.289
Attacks against availability	Availability	5.252
Supplier looking at sensitive data	Confidentiality	5.231
Disclosure of data by the provider	Confidentiality	5.063
Disclosure of internal system data	Confidentiality	5.046
Network performance problems	Performance	4.889
Unintentional downtime	Availability	4.796
Eavesdropping communications	Confidentiality	4.707
Insufficient logging of actions	Accountability	4.669
Proprietary technologies	Maintainability	4.630

Table 3.21 shows descriptive statistics of the ten highest rated IT security risks related to Cloud Computing. It can be seen that all four identified confidentiality-related risks are included. Interestingly, none of the five integrity risks is among the ten risks perceived to be most serious, even tough the rarely used term "integrity" was not used in the risks' descriptions. We paraphrased the term with deliberate "manipulation" or accidental "modification" of data (see appendix A.5).

It is remarkable that two of the top ten security risk items assume that the provider deliberately shows misconduct: the risk that the supplier is looking at sensitive customer data stored or processed on its servers (e. g., Beulen et al., 2005; Briscoe and Marinos, 2009; Schwarz et al., 2009), and the risk that data are disclosed by the provider to unauthorized third parties (e. g., Itani et al., 2009; Kaufman, 2009; Viega, 2009). As these risks cannot be fully mitigated by technical countermeasures, this stresses the need of trust building measures issued by Cloud Computing providers.

The risk of "Proprietary technologies" was rated to be a serious risk by the IT executives, although analysis in section 3.6 shows that it has no significant impact on the adoption decisions. This means that even though Cloud Computing users know that proprietary technologies increase lock-in effects, it does not affect their attitudes towards the technology. This has implications for providers which can use own formats or protocols to their advantage by binding customers to their products (Buxmann et al., 2011a, pp. 28f. and 33f.).

The strong relation between perceived IT security risk and the intention to increase adoption is an important theoretical contribution to the IT security and IT risk literature. Although it has been shown that there are many factors influencing the adoption decision of potential customers and users, such as subjective norm (Fishbein and Ajzen, 1975), perceived benefits (Chwelos et al., 2001) and opportunities (Gewald and Dibbern, 2009), as well as other types of risk, e. g., economic and strategic risk (Benlian and Hess, 2011), perceived IT security risk, in and of itself, explains 28% of the dependent variable's variance (see figure A.9 in appendix A.8).

Additionally, the results of this thesis shed light on the dual detrimental role of PITSR. The theoretical model proposed in figure 3.8 links perceived IT security risk with both positive and negative attitudinal evaluations to fully comprehend PITSR's impact in a broader nomological network. Analysis shows that the six different dimensions of IT security risk can, at the same time, both increase reservations against Cloud Computing (e. g., due to data losses and extended downtimes) and decrease the promised opportunities of Cloud Computing adoption (e. g., through cost advantages and switching flexibility). Therefore, those security risks not only nurture the perceived negative utility but also abate the perceived positive utility of Cloud Computing, and, thus, may exhibit a double detrimental effect on the adoption intentions related to Cloud Computing.

The perceived positive utility of Cloud Computing adoption has a stronger influence on IT executives' intention to increase the level of Cloud Computing than the perceived negative utility. This is in line with previous studies where the perceived opportunities had a substantially stronger impact on the intention to increase the level of adoption than perceived risks (Gewald and Dibbern, 2009; Benlian and Hess, 2011).

The CSA-based analysis in sections 3.5 and 3.6 shows that confidentiality-related risks are most influential, followed by availability and accountability risks. These three dimensions of IT security risks show highly significant effects on PITSR as well as on the (potential) users' adoption intentions. The other three dimensions, i. e., performance, maintainability, and integrity, are significant but with a lower effect on PITSR and the intention to increase the level of Cloud Computing adoption. Even though integrity risks are rated higher on average than performance and maintainability risks, they seem to have less impact on forming the aggregated perceived IT security risk.

Chapter 4
Risk Quantification Framework

In this chapter about the risk quantification framework[1], first, the model – including its parameters as well as related equations and algorithms – is introduced. The model supports risk management by efficiently aggregating the individual risks for the decomposed parts of an IT scenario back to an overall risk. The second section describes simulation results regarding sensitivity analysis, identification of cost drivers, and the introduction of inaccuracy. Third, the application of the proposed risk quantification framework using a real-life business process and a prototype of a SaaS-based implementation are presented.

4.1 Model Description

The framework is build around the thought that – especially for larger IT architectures – it is hard to manage all involved risks using only a high level perspective. As the complexity of large-scale systems is too high, the model facilitates decomposition of scenarios into smaller parts, i. e., smaller scenarios for which the IT risk management process can be carried out more easily. Especially during the phases of risk identification and quantification, decision makers can, thus, better analyze and estimate potential risks. The risk quantification framework supports risk quantification by efficiently aggregating the individual risks for the decomposed parts back to an overall risk distribution.

Each scenario is assumed to consist of various components of different types. Expert interviews with IT risk management consultants showed that scenarios involving IT outsourcing are usually composed of services and data transfers. Using

[1] Compare, in the following, Ackermann and Buxmann (2010); Ackermann et al. (2013).

T. Ackermann, *IT Security Risk Management,* DOI 10.1007/978-3-658-01115-4_4,
© Springer Fachmedien Wiesbaden 2013

visualizations such as the one shown in figure 4.1 help to better identify and quantify the most critical data transfer-related risks, when data are transferred from one service of "security zone" (e. g., an in-house service) to another "security zone" (e. g., a service hosted by an external provider).

All of the risks, found in the conducted literature review (see section 3.1 as well as tables A.1 and A.2) could be assigned to either services or data transfers. There were no risks that are neither related to services nor to data transfers. Therefore, in the following, we speak of scenarios consisting of services and data transfers. Nonetheless, the proposed model allows incorporation of other types of scenario components, such as people or devices.

In order to quantify risks of a given scenario and in order to calculate the risk measure characteristics with which the scenario's cost drivers can be analyzed, the distribution of potential losses has to be calculated.

Our approach uses the business process with its risk parameter tables as an input for the calculation. The model parameters, i. e., the variables used to describe a scenario (e. g., a distributed business process) are described in section 4.1.1, while two different approaches for calculating the distribution of potential losses is described in section 4.1.2. In section 4.1.3, algorithms for deriving risk measures are presented.

The result is presented in the form of a discrete Probability Density Function of the Potential Losses (PDFL). See figures 4.2 and 4.15 for examples of such functions. Based on this distribution, risk measure characteristics can be derived using calculations provided in section 4.1.3.

4.1.1 Parameter Descriptions

In this section, all input variables of the model are successively introduced and described. Sections 4.1.1.1 and 4.1.1.2 present the basic parameters, needed for every scenario, while sections 4.1.1.3 to 4.1.1.5 present various possible extensions to the base model.

4.1.1.1 Basic Scenario Parameters

In the previous section, a scenario was described to be composed of services and data transfers. More generally, we say that a scenario consists of component types, such as services and data transfers. The set X contains all valid scenario component types, e. g., $X = \{S; T\}$. This states that a scenario consists of two different type: services (S) and data transfers (T). Figure 4.1 visualizes an exemplary scenario

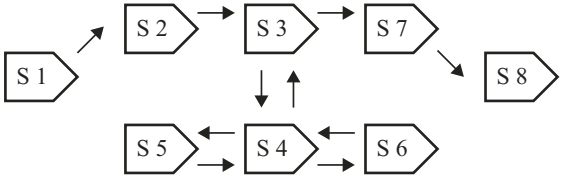


Figure 4.1 Exemplary Service Graph. The nodes represent services, the connections represent data transfers.

of a business process consisting of two different scenario component types, i. e., services and data transfers. The nodes of the graph represent the eight services, while ten data transfers between the services are indicated by the graph's edges.

The set of all scenario component types X has been introduced in order to be able to incorporate other abstract types of components that could be important to risk quantification of IT-related scenarios, such as companies, devices, or people. Additionally, this form allows shorter equations and algorithms because it is no longer necessary to explicitly incorporate separate service and data transfer related calculations.

The individual scenario components are stored in sets called K^x, where x indicates the service component type. E. g., if X was defined as above, all of the scenario's services are contained in the set K^S while all data transfers are contained in K^T. For the business process shown in figure 4.1, the sets could be defined as $K^S = \{S1;\ldots;S8\}$ and $K^T = \{T1;\ldots;T10\}$.

4.1.1.2 Basic Risk Parameters

The invocation of services is associated with service-related risks. p^S_{rk} denotes the occurrence probability of service-related risk r in service k. An incident of service-related risk r (occurring in one or more of the service calls) causes costs of c^S_r. Additionally, every data transfer k between two services is associated with data transfer-related risks r with an occurrence probability p^T_{rk} and caused costs of c^T_r. The model is based on the assumption that all risks are uncorrelated. This implies that all analyzed risks should be mutually exclusive (see, e. g., Wang et al. (2008, pp. 108f.) for a similar assumption).

If only these basic risk parameters are used to model a scenario, it is possible to calculate the aggregated risk occurrence probabilities $\bar{p}^x_r$ for each risk r like shown in equation (4.1).

Table 4.1 Input Variable Definitions for the Simulation Model

Variable	Domain	Description
S		Set of services
T		Set of data transfers
X		Set of service process component types, e. g., $X = \{S; T\}$
x	$\in X$	Represents one type of service process components, such as services (S) or data transfers (T)
K^x		Set of all components of service process component type x
k	$\in K^x$	Represents one component, e. g., one individual service or a single data transfer
R^x		Set of all risks, related to service process components of type x
r	$\in R^x$	Represents one risk
p_r^x	$\in [0;1]$	Global occurrence probability of risk r related to service process components of type x
p_{rk}^x	$\in [0;1]$	Occurrence probability of risk r related to service process components of type x in component k
c_r^x	$\in \mathbb{R}^+$	Potential global losses associated with risk r related to service process components of type x
c_{rk}^x	$\in \mathbb{R}^+$	Potential losses associated with risk r related to service process components of type x in component k
d_k^x	$\in \mathbb{R}$	Number of invocations of component k related to service process component type x
f_r^x	$\in \mathbb{B}$	Boolean flag which indicates whether the d_k^x are taken into account for risk r related to service process component type x

$$\bar{p}_r^x := 1 - \prod_{k \in K^x} (1 - p_{rk}^x) \tag{4.1}$$

This probability determines the chance that risk r will occur at least once in the whole scenario. It is derived by calculating the probability for the event that the risk does not arise in any service or data transfer k and then using the complementary probability.

4.1.1.3 Extension 1: Advanced Workflow Patterns

In order to map business processes using advanced workflow patterns, such as loops and branches, for each risk, we introduce a flag f and a parameter d, for each service or data transfer. If f is true, the number of invocations d_k^x of component k

is taken into account when the overall risk occurrence probability is calculated. This means that a service which is called twice leads to a higher chance of risk occurrence while a service which is only called one out of ten times, leads to a lower probability compared to exactly one invocation. Per default, all d_k^x are 1.0 and all flags f_r^x are set to false. If the transition probabilities for all conditional branches of a workflow are given, the d parameter values can easily be calculated by solving a system of linear equations (Ross, 1996).

While some risks, such as inflexible contracting, are related to the provider, other risks, such as eavesdropping using Man-in-the-Middle attacks, could occur in every single data transfer (Schneier, 2004). Therefore, it is important to be able to model loops and branches. This allows modeling business processes that iterate over a set of customers or products, where a subset of the services is called multiple times. Additionally, branches are necessary in order to model optional services which are not invoked every time the workflow runs, for example, because they are charged on a pay-per-use basis.

If flag f for a service- or data transfer-related risk is set, the number of invocations of the component k, d_k^x, is incorporated into the calculation of the combined and aggregated occurrence probability $\bar{p}_r^x$ of risk r for scenario component type x as follows:

$$\bar{p}_r^x := 1 - \prod_{k \in K^x} \left((1 - p_{rk}^x)^{d_k^x} \right) \tag{4.2}$$

If flag f_k^x is not set, equation (4.2) remains the same except the exponent d_k^x, which is then considered to be 1.0 and can therefore be omitted for faster calculations.

4.1.1.4 Extension 2: Dependent Losses

Additionally to static losses c_r^x, it is also possible to model losses c_{rk}^x which only arise, if the risk occurs at a specific component k. These costs depend on the affected services or data transfers and allow modeling scenarios where the potential losses are higher if two services are affected by a risk simultaneously. The default individual costs c_{rk}^x are zero.

Dependent losses occur, for example, if downtime of one service is more critical than non-availability of others, e. g., because there might be no fallback-services or because it might take longer to recover in certain cases. Another example are replay attacks (Biskup, 2009): It might be harmless if a valid data transmission is fraudulently repeated to a service that just performs the task of validating data.

Conversely, an order service accepting maliciously repeated order messages could lead to complete disorder of a supply chain.

The calculation can be modeled to be a new instance of the base problem: Each service or data transfer is modeled to be a new risk with its specific costs c^x_{rk} and overall occurrence probability p^x_{rk}. After calculating the joint probability density function (see section 4.1.2.2), all cost values of this distribution except the costs equal to zero are increased by the global costs c^x_r.

Please note that, if there is a service or data transfer with individual costs of zero and an occurrence probability greater zero, it is necessary to keep track of when the risk did and did not occur, because later the global costs need to be added to only the cases where it occurred.

4.1.1.5 Extension 3: Conditional Probabilities

For some risks, it may be necessary to define a global event whose occurrence influences the probabilities that the risk occurs in the individual services or data transfers. Examples for these events can be that a used security mechanism (e. g., an encryption algorithm) suddenly becomes insecure or a fire in the local data center which affects internal services. Therefore, for each risk r, we introduce a parameter p^x_r which defines the occurrence probability of the global event. If the event does not occur, all p^x_{rk} are treated to be 0.0. If the event occurs, the p^x_{rk} define the chance of risk occurrence. This property is connected to conditional independence and closely related to the concept of divergent Bayes nets. The default value for the event-related global probabilities p^x_r is 1.0.

An example of such a global event may be that insufficient separation of co-existing Virtual Machines (VMs) in a Cloud Computing infrastructure can be exploited. This would increase the chances that attackers on the same system can access other VMs' virtual disks or memory without authentication. Furthermore, it could lead to confidentiality risks, such as data leakage, but could also be a threat to integrity in case of unauthorized data modifications (Dawoud et al., 2010).

The conditional probabilities can be incorporated before the calculation of the overall risk occurrence probabilities, by multiplying the individual service- or data transfer-related occurrence probabilities p^S_{rk} and p^T_{rk} with the global occurrence probabilities p^S_r and p^T_r.

4.1.2 Calculations of the Overall Risk Distribution

The following two sections describe two different approaches for calculating the overall probability density function of the potential losses. Both approaches will be compared in section 4.2.3.

4.1.2.1 Power Set-Based Approach

A first approach to calculate the costs' probability density function is based on the power set $\mathscr{P}$ of all risks. This approach relies on the aggregated risk occurrence probabilities $\bar{p}_r^x$ which means that it is not possible to use individual losses per scenario component (see section 4.1.1.4). The process of calculation the overall probability density function PDFL consists of the following steps:

1. Aggregate the individual occurrence probabilities p_{rk}^x to the aggregated risk occurrence probabilities $\bar{p}_r^x$ for each risk r using equation (4.1)
2. Calculate the overall PDFL using the power set-based approach using listing 4.1

Listing 4.1 represents the most basic form of the algorithm, as it only allows basic risk parameters defined in section 4.1.1.2. The algorithm does not yet incorporate advanced workflow patterns (see section 4.1.1.3) and conditional probabilities (see section 4.1.1.5).

The algorithm iterates over all possible combinations of risks that could occur simultaneously (line 3). For each combination the probability and the arising costs are calculated (lines 6 to 13) and added to the probability density function of the potential losses PDFL (lines 14 to 18) which maps costs to their occurrence probability (Ackermann and Buxmann, 2010, p. 5).

Each subset in the power set $\mathscr{P}$ represents one possible combination of risks $\in \{(X;R^x) \mid x \in X\}$ that can occur together. The computation can, e. g., be implemented using a bit representation for iterating over all items in the power set. If a bit is one, the associated risk occurs, if it is zero, the risk does not occur. In total, there is one bit for each of the R risks. As the algorithm iterates over all integers from zero to $2^R - 1$, all 2^R possible combinations of risks that can occur together can be analyzed.

For each bit configuration, the algorithm performs $R-1$ multiplications in order to calculate the aggregated risk occurrence probability $\bar{p}_r^x$ using equation (4.1). In summary, this leads to $2^R \cdot (R-1)$ multiplications. Regardless of the probability and cost values, the number of multiplications remains the same.

This approach, however, has some disadvantages. For every added risk, more than twice as many multiplications have to be calculated. Additionally, because of

```
input   p̄_r^x ; c_r^x ∀ (x;r) ∈ {(X;R^x) | x ∈ X}
output  PDFL: the calculated probability density function of the potential losses
for each subset ∈ 𝒫({(X;R^x) | x ∈ X})
    costs ← 0.0
    probability ← 1.0
    for each (x;r) ∈ {(X;R^x) | x ∈ X}
        if (x;r) ∈ subset then
            costs ← costs + c_r^x
            probability ← probability · p̄_r^x
        else
            probability ← probability · (1.0 − p̄_r^x)
        end if
    end for
    if ∃ PDFL[costs] then
        PDFL[costs] ← PDFL[costs] + probability
    else
        PDFL[costs] ← probability
    end if
end for
return PDFL
```

Listing 4.1 Calculation of the Potential Losses' Probability Density Function

the used bit representation, the algorithm scales only to the number of bits available per integer or long, which means that, in most cases, more than 64 risks cannot be handled.

Furthermore, it can be shown that $2^{R-1} \cdot (R-2)$ multiplications are unnecessarily repeated. For a large number of risks, the ratio of unnecessarily repeated multiplications to the total number of multiplications approaches 50%, which is shown in equation (4.3).

$$\lim_{R \to \infty} \frac{2^{R-1} \cdot (R-2)}{2^R \cdot (R-1)} = \frac{1}{2} \tag{4.3}$$

This means that using the power set-based approach, a sufficiently large number of risks cannot – or only with great difficulty – be taken into account. Moreover, research on IT outsourcing increasingly identified more and more risks over the last couple of years. For example, Earl (1996) lists eleven risks, Lacity et al. (2009) presents a collection of 28 risks, and Ackermann et al. (2011) identified 70 technological risks of IT outsourcing.

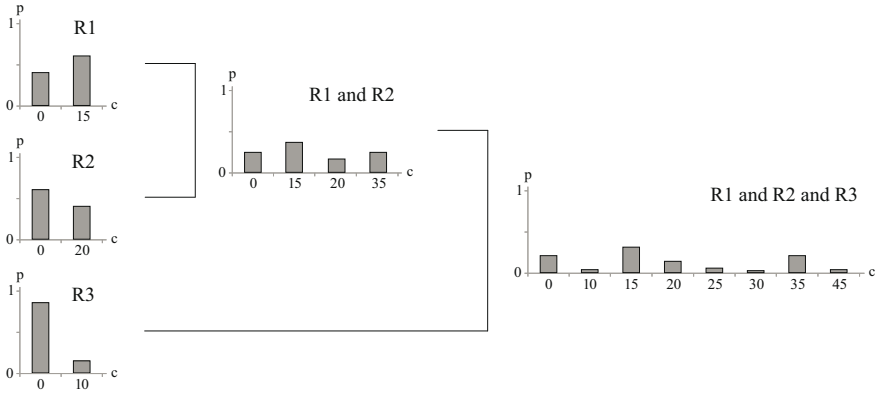


Figure 4.2 Calculation of the Joint Density Function Without Rounding

4.1.2.2 Hierarchical Approach

A more efficient approach, which allows implicit caching of these multiplications, is to divide the problem into smaller sub-problems. Like shown in figure 4.2, it is possible to calculate joint probability density functions by successively joining two probability density functions. The hierarchical approach which we propose starts with simple distributions for each risk, like shown in figure 4.2 at the left side: No costs occur with probability $(1-p)$ and costs c with probability p. The process of calculation the overall probability density function PDFL consists of the following steps:

1. Calculate separate PDFLs for each individual risk r
2. Iteratively combine all separate PDFLs to the final PDFL

The approach computes joint distributions until only one distribution, the final density function, remains. For R risks, $(R-1)$ joins need to be calculated. We use a priority queue for storing all distributions sorted by the number of cost values on the x-axis. The approach always combines the two smallest distributions in order to keep the number of multiplications to a minimum and to create the smallest possible distributions for the next steps in the hierarchy. If the distributions were simply joined successively, the hierarchies would not be as shallow and balanced, which would lead to a higher number of multiplications. Exemplary hierarchies for scenarios with 9 and 16 risks are shown in figure 4.3.

Additionally, the partitioning of the calculation is more flexible compared to previously proposed models, because it is possible to start with distributions that contain more than two values on the x-axis in the first step. This allows incor-

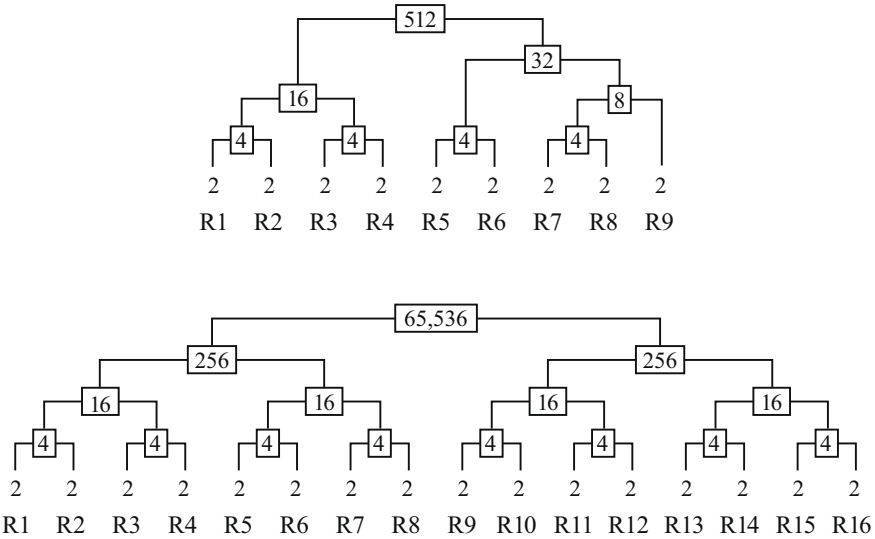


Figure 4.3 Tournament Complexity

poration of risks whose losses depend on the affected services or data transfers risks (see the model's extension with dependent losses in section 4.1.1.4), as these special kind of risks lead to initial distributions with multiple cost values on the x-axis.

As it is complicated to estimate the number of multiplications for this kind of hierarchy, we calculate an upper bound by assuming the worst case where all distributions are successively joined regardless of their size. The calculation would look like follows: ((R1 and R2) and R3) and R4 ... which leads to high and unbalanced hierarchies. The number of multiplications can then be recursively defined as $g(R) = g(R-1) + 2 \cdot R$ or iteratively calculated like shown in equation (4.4):

$$\sum_{i=2}^{R} 2^i = \left(\sum_{i=0}^{R} 2^i \right) - 3 = \left(2^{(R+1)} - 1 \right) = 2^{(R+1)} - 4 \tag{4.4}$$

Compared to the number of multiplications of the power set-based algorithm, $2^R \cdot (R-1)$, even in the worst case, the hierarchical approach needs fewer multiplications (for $R \geq 2$). If the approach always joins the two smallest (i. e., with the fewest number of cost values on the x-axis, such as shown in figure 4.3) distributions, the differences will be even greater.

An alternative approach for faster calculation of joint density functions is shown by Sang et al. (1992). They compute the joint density function of a set of discrete independent random variables by generating the resulting distribution in order of decreasing probability. This allows the algorithm to stop the calculation as soon as a given accuracy has been obtained.

4.1.3 Determination of Risk Measures

Based on the calculated discrete probability density functions, the PDFLs, described in sections 4.1.2.1 and 4.1.2.2, it is possible to derive risk measures. These characteristics of the risk distribution can be incorporated into individual utility-functions and, thus, be used to evaluate scenarios. For example, a risk neutral decision maker solely tries to minimize the mean value μ of the potential losses. In this section, we describe how to calculate three basic risk measures, i. e., the average μ (also mean or expected value), the variance σ^2, and the Value-at-Risk. For other risk measures, such as the expected shortfall, based on loss distributions see McNeil et al. (2005, pp. 35–48). A basic algorithm for calculating the average is given in listing 4.2.

```
1 input   PDFL
2 output  The calculated average μ of the potential losses
3 ret ← 0.0
4 for each k ∈ PDFL.getCostValues()
5     ret ← ret + (PDFL[k] · k)
6 end for
7 return ret
```

Listing 4.2 Calculation of the Average Potential Losses

The algorithm simply iterates (line 4) over all cost values on the distribution's x-axis and builds the sum of all weighted averages by multiplying each cost value with their occurrence probability (line 5). Finally, listing 4.2 returns the expected value for the given discrete costs' probability density function PDFL.

```
1  input    PDFL
2  output   The calculated variance σ² of the potential losses
3  xs ← PDFL.getCostValues()
4  iterator = xs.iterator()
5  m ← iterator.next()
6  sumw ← PDFL[m]
7  t ← 0.0
8  while (iterator.hasNext())
9      xi ← iterator.next()
10     wi ← PDFL[xi]
11     q ← xi - m
12     temp ← sumw + wi
13     r ← q · wi / temp
14     m ← m + r
15     t ← t + r · sumw · q
16     sumw ← temp
17 wend
18 return t
```

Listing 4.3 Calculation of the Variance of the Potential Losses

Listing 4.3 uses an advanced version for calculating the distribution's variance (i. e., the square of the standard deviation σ) for the given discrete costs' probability density function PDFL. Normally, the variance is calculated by first calculating the average μ and then calculating the squared deviation of the distribution from its expected value in a second step. This process would require two iterations over all cost values on the x-axis of the PDFL, and, thus, consume more time.

Therefore, an advanced process for calculating the variance σ^2 in one iteration instead of two is used. The calculation is based on the "WV2 Proposed Algorithm for Weighted Variance" by West (1979) in one pass. The algorithm stores all weights as occurrence probabilities in the variables called wi, while the xi store the cost-related values. The mean, which is continuously updated, is stored in variable m.

After calling the function, the standard deviation σ can be derived by taking the square root of the calculated variance σ^2.

The Value-at-Risk is defined as the lowest number l, so that the probability that losses L greater than l occur, is exceeded by $(1-\alpha)$ (Duffie and Pan, 1997). A mathematical definition is given by McNeil et al. (2005, p. 38):

$$\mathrm{VaR}_\alpha := \inf\{l \in \mathbb{R} : P(L > l) \leq 1-\alpha\} \tag{4.5}$$

$$:= \inf\{l \in \mathbb{R} : F_L(l) \geq \alpha\} \tag{4.6}$$

```
1  input    Confidence level α ∈ {r ∈ ℝ | 0 < r ≤ 1} ; PDFL
2  output   The calculated Value-at-Risk
3  maxProbabilityOfError ← 1.0 − α
4  currentProbabilityOfError ← 0.0
5  sortedCosts ← PDFL.getSortedCostValues()
6  backwardsIterator ← sortedCosts.descendingIterator()
7  lastCosts ← sortedCosts.getSortedCostValues().last()
8  while (
9          backwardsIterator.hasNext() &&
10         currentProbabilityOfError \leq maxProbabilityOfError)
11     currentCosts ← backwardsIterator.next()
12     currentProbabilityOfError ← currentProbabilityOfError +
13             PDFL[currentCosts]
14     lastCosts ← currentCosts
15 wend
16 return lastCosts
```

Listing 4.4 Calculation of the Value-at-Risk

The characteristic represents a threshold value which specifies the maximum amount of losses that will occur with a given confidence level α. This means that all losses greater than this threshold are less likely than $(1-\alpha)$. Usually, the Value-at-Risk is a statistical measure of the risk associated with an investment or set of investments, based on extreme value theory. It quantifies the stochastic behavior at unusually large (or small) levels and is, thus, concerned with occurrence probabilities and statistical questions related to those extremely rare events (Wang et al., 2008, p. 106).

Listing 4.4 returns the Value-at-Risk for the given discrete costs' probability density function (PDFL) and the given confidence level α. For performance reasons, the calculation is done from the highest to the lowest cost values on the distribution's x-axis. Therefore, the algorithm is more efficient for higher confidence levels (i. e., greater 0.5).

The algorithm starts with the highest possible amount of losses that can occur and then iterates back to the lowest possible amount on the distribution's x-axis. The iteration (lines 8 to 15) stops, when the given confidence level is reached, i. e., when the sum of all visited probabilities is greater than $(1-\alpha)$. This means that all the following cost-related values (to the left of the reached threshold) occur with a probability $\geq \alpha$.

4.2 Simulations

The following sections present various simulation-based results regarding the proposed model. First, we show how cost drivers in a given scenario can be identified. Second, we analyze the effect of the input parameters using a sensitivity analysis. The third section presents and further analyzes the trade-off between the expenditure for the elicitation of input data and the accuracy of the obtained results.

4.2.1 Identification of Costs Drivers

Based on the model parameters, the contribution to the aggregated distribution of potential losses can be identified for each risk separately. It is possible to create R new scenarios based on the given complete scenario with R risks, where each new scenario consists of only one risk. Because this risk is either related to the services or the data transfers, each new scenario only needs to contain either the services or data transfers of the complete scenario. This corresponds to the potential losses of a single row in the table containing all scenario parameters. The distribution of potential losses can then be calculated like it is described in section 4.1.2.2.

The result itself is, again, a discrete probability density function which maps cost values to their occurrence probabilities and which can be analyzed and assessed using the same methods as the overall distribution of potential losses.

If appropriate risk measures are used for the assessment, it is possible to show how the aggregated risk is concentrated in the individual risks, as a fraction of the overall risk. The following equations show that the μ-σ-characteristic of the overall distribution $(X+Y)$ equals the sum of individual μ-σ-characteristics of the individual distributions X and Y:

$$a \cdot E(X+Y) + b \cdot Var(X+Y) \tag{4.7}$$
$$= a \cdot [E(X) + E(Y)] + b \cdot [Var(X) + Var(Y)] \tag{4.8}$$
$$= a \cdot E(X) + a \cdot E(Y) + b \cdot Var(X) + b \cdot Var(Y) \tag{4.9}$$
$$= a \cdot E(X) + b \cdot Var(X) + a \cdot E(Y) + b \cdot Var(Y) \tag{4.10}$$

This means that it is possible to calculate the μ-σ-characteristic for all risks individually and then calculate the overall μ-σ-characteristic by just building the sum. This can be done much faster than calculating the overall probability density function and then calculating the μ-σ-characteristic. Therefore, if a decision maker is only interested in μ and σ of the overall distribution, it is possible to calculate

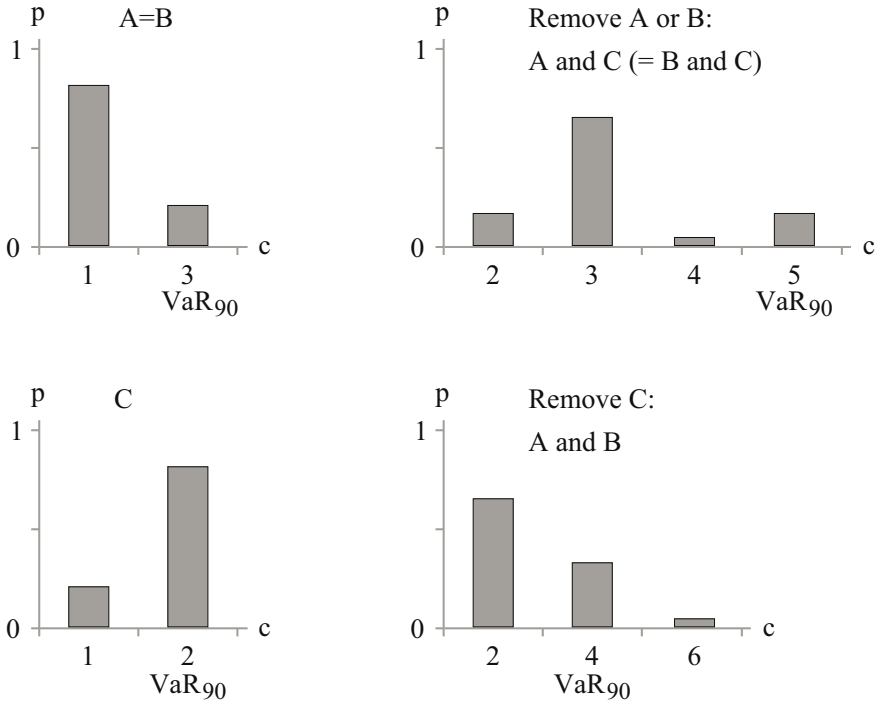


Figure 4.4 Example for the Violated Additivity of the Value-at-Risk

these two characteristics for scenarios consisting of millions of risks, services, and data transfers, because the expensive calculation of the overall probability density function, with its exponential runtime complexity, can be omitted.

This additivity of the μ-σ-characteristics allows identifying the individual risk that introduces the largest fraction of the overall risk. If this risk cost driver is eliminated (e. g., by implementing countermeasures that lower the occurrence probability to zero) the overall μ-σ-characteristic will decrease by the risk's individual characteristic.

This, however, cannot be done, if the Value-at-Risk is used as risk measure, as the quantile-based Value-at-Risk is known to violate the property of additivity in general (Daníelsson et al., 2005). This means that it is not possible to add up the individual Value-at-Risk of all risks in order to calculate the Value-at-Risk of the overall scenario. The sum does not even have to be smaller than the Value-at-Risk of the overall scenario, which means that the Value-at-Risk is not even subadditive (McNeil et al., 2005, p. 40).

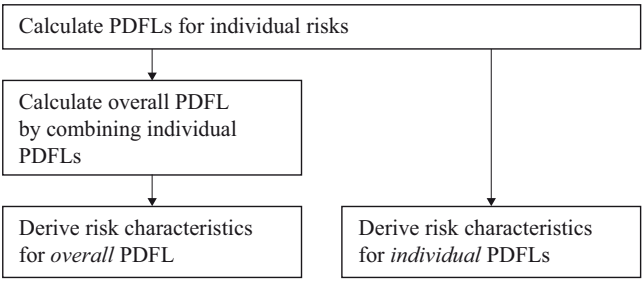


Figure 4.5 Process of Deriving Risk Characteristics

Therefore, it is not possible to use the Value-at-Risk in order to identify the risk whose removal would lead to the largest reduction of the overall Value-at-Risk, like the following small counterexample, consisting of three risks, shows (see figure 4.4).

Risk A and risk B are identical: potential losses of 1 occur with a probability of 80% and costs of 3 with probability 20%. Both risks have a Value-at-Risk ($\alpha = 0.9$) of 3. Risk C leads to losses of 1 and 2 with chances 20% and 80% (Value-at-Risk: 2). If risks A or B are removed, the resulting overall distribution has a Value-at-Risk of 5, while removal of risk C (with its smaller individual Value-at-Risk) leads to a larger reduction and a resulting Value-at-Risk of 4.

Similar to identification of cost drivers at the risk level, it is possible to identify a single service's or data transfer's contribution to the overall probability density function. This corresponds to the potential losses of a single column in the table containing all scenario parameters. See tables 4.6 and 4.7 for an example of two of these parameter tables. Using these "vertical slices" of the parameter tables allows decision makers to identify the critical and most risky components of a given scenario. Thereby, it is possible to detect services that could be replaced by more secure, alternative services offering the same functionality. Similarly, these "vertical slices" allow to check for data transfers which could be further secured, e. g., by additional encryption mechanisms.

Finally, the described approach can be applied to single cells in the tables that contain all scenario parameters. For each combination of services/data transfers and risks, the result will always be a relatively simple distribution with just two discrete cost values on the x-axis: No costs occur with probability $(1 - p_{ij})$ and costs $c_{ij} + c_i$ with probability p_{ij}.

This way, for example, it is possible to compare the potential losses of a specific risk, such as eavesdropping information, in a specific data transfer, to the potential losses due to breakdown of a certain service.

An application of these techniques can be seen when the proposed risk quantification framework is applied to a real life scenario in section 4.3.1.4. Figure 4.5 illustrates the steps of the calculation process and shows that derivation of risk characteristics for individual risks does not involve the computationally expensive step of calculating the overall PDFL by combining all individual PDFLs.

4.2.2 Sensitivity Analysis

In order to obtain an initial estimate of how the model's parameters affect the calculated probability density functions, we fix the values of all parameters except one and make simulation runs for varying levels of the "free" parameter (Law and Kelton, 2000). Using this approach, it is possible to see how the derived characteristics, μ, σ, and the Value-at-Risk, respond to changes in a single parameter.

An important factor that influences the distribution of potential losses is the aggregated risk occurrence probability $\bar{p}_r^x$ shown in equation (4.1). If the individual occurrence probabilities p_{rk}^x were fixed, e. g., to 0.5, the calculated $\bar{p}_r^x$ would strongly depend on the number of services and data transfers. For $p_{rk}^x = 0.5$, the aggregated $\bar{p}_r^x$ of the risk to occur would be equal to or greater than 50%, 75%, 90%, 99%, and 99.9% for 1, 2, 4, 7, and 10 service components. Even for $p_{rk}^x = 0.1$, the aggregated occurrence probability $\bar{p}_r^x$ would be larger than 90% for more than 21 services or data transfers. In order to exclude this effect, based on the proof shown in equations (4.11) to (4.18), the p_{rk}^x were not randomly drawn from $[0;\ 1]$ but from $[0;\ 2 \cdot \left(1 - \sqrt[|K^x|]{1 - \hat{p}_r^x}\right)]$. Using this formula, it is possible to specify the resulting $\hat{p}_r^x$ regardless of the number of service components in the scenario. Please note that this only holds true, if the parameter for the number of service or data transfer invocations d_k^x is not used for all components of the scenario.

In the following, we use a simplified notation, where $|K|$ denotes the number of components in a scenario and $\hat{p}$ the targeted expected aggregated occurrence probability for all risks. Additionally, we assume that all occurrence probabilities are equal to p', the *adjusted* occurrence probability defined in equation (4.11). The *calculated* aggregated occurrence probability for all risks $\bar{p}$ (see equation (4.12); defined in equation (4.1)) can then be shown to be equal to the *specified* aggregated risk occurrence probability $\hat{p}$:

Table 4.2 Parameters used in Sensitivity Analysis

Variable	Default Value
Number of services $\left\|K^S\right\|$	500
Number of data transfers $\left\|K^T\right\|$	500
Cost values c_r^x	$\in [1;\ 1{,}000]$
Expected aggregated probability $\hat{p}_r^x$	0.5
Number of iterations I	1,000
Value-at-Risk Confidence α	0.9

$$p' := 1 - \sqrt[|K|]{1-\hat{p}} \tag{4.11}$$

$$\bar{p} = 1 - \prod_{k \in K} \left(1 - p'\right) \tag{4.12}$$

$$= 1 - \left(1 - p'\right)^{|K|} \tag{4.13}$$

$$= 1 - \left(1 - \left(1 - \sqrt[|K|]{1-\hat{p}}\right)\right)^{|K|} \tag{4.14}$$

$$= 1 - \left(1 - 1 + \sqrt[|K|]{1-\hat{p}}\right)^{|K|} \tag{4.15}$$

$$= 1 - \left(\sqrt[|K|]{1-\hat{p}}\right)^{|K|} \tag{4.16}$$

$$= 1 - (1 - \hat{p}) \tag{4.17}$$

$$= \hat{p} \tag{4.18}$$

If not stated otherwise, all simulation runs have been carried out using the following parameter values: the number of scenario components has been fixed to 1,000, i. e., $\sum_{x \in X} |K^x| = \left|K^S\right| + \left|K^T\right| = 500 + 500 = 1{,}000$, the cost values c_r^x have been randomly drawn from $[1;\ 1{,}000]$ (therefore, the fixed expected aggregated cost of risk r, $\hat{c}_r^x = 500.5$). $\hat{p}_r^x$, the expected aggregated risk occurrence probability, was fixed to be 0.5 so that each risk, regardless of the number of service components, had a chance of 50% to occur or not. The Value-at-Risk was calculated with a confidence $\alpha = 0.9$. For each data point, we created 1,000 random scenarios, based on these parameters. Figures 4.6 to 4.8 are therefore based on 81,000, 135,000 and 135,000 calculated probability density functions. Table 4.2 lists the default values.

Figure 4.6 shows that the Value-at-Risk (with α = 0.9) exceeds the expected value (μ) as well as the standard deviation (σ), and that the difference between μ and the Value-at-Risk gets bigger with every added risk. All three curves grow

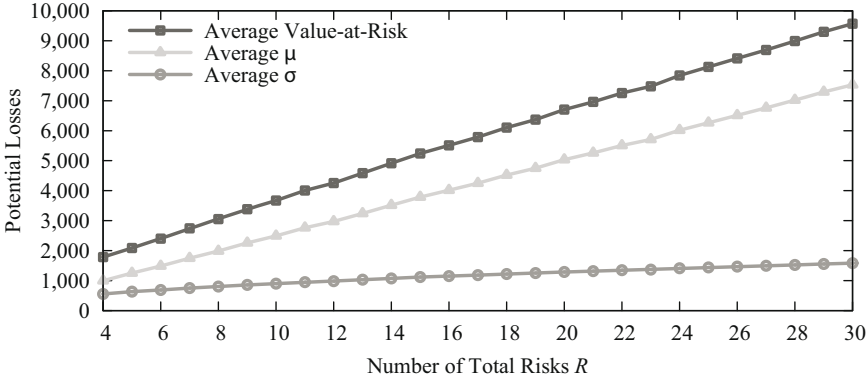


Figure 4.6 Potential Losses Plotted Against the Number of Total Risks

linearly with the number of total risks R. The measured average μ of potential losses can be approximated using equation (4.19):

$$\text{Average } \mu \approx \sum_{(x;r)\in\{(X;R^x)\ |\ x\in X\}} \bar{p}_r^x \cdot \bar{c}_r^x \tag{4.19}$$

This means that every added risk increases μ by its expected aggregated occurrence probability $\bar{p}_r^x$ times its expected overall losses $\bar{c}_r^x$. If we would have used fixed *individual* occurrence probabilities p_{rk}^x instead of fixed *aggregated* occurrence probabilities $\hat{p}_r^x$ for the sensitivity analysis simulations in this section, all risks r would have occurred with $\bar{p}_r^x = 1.0$ because of the large number of services and data transfers (i. e., $\left|K^S\right| + \left|K^T\right| = 1{,}000$):

$$\bar{p}_r^x = 1 - \prod_{k\in K^x} (1 - p_{rk}^x) = 1 - \prod_{k\in K^x} (1 - 0.5) \tag{4.20}$$

$$= 1 - (1 - 0.5)^{|K^x|} = 1 - 0.5^{500} \tag{4.21}$$

$$\approx 1 - 3 \times 10^{-151} \approx 1 - 0 = 1 \tag{4.22}$$

Since losses are the central object of IT risk management, in consequence, they should be incorporated into the decision process in order to get an accurate picture of a scenario (McNeil et al., 2005, p. 35). Figure 4.6 shows that risk-neutral decision makers loose information by only looking at the mean value of potential losses and, therefore, neglecting the variance in the distribution of potential losses. Instead of using only the μ-characteristic, risk management should be interested

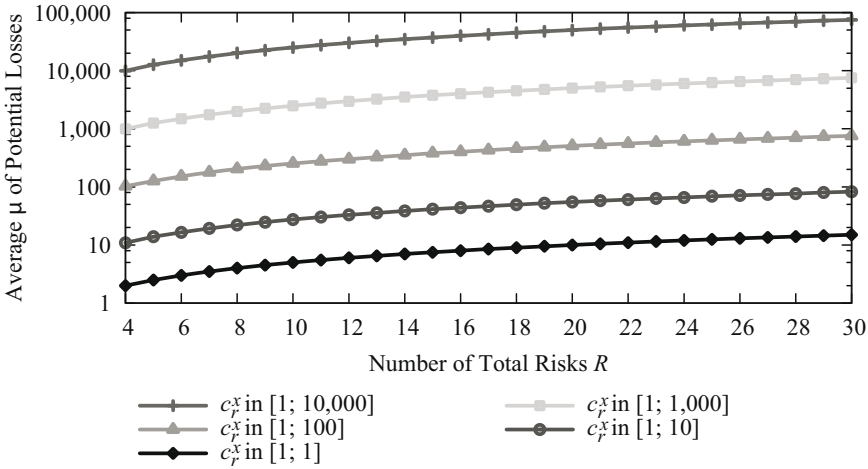


Figure 4.7 Average Potential Losses Depending on the Magnitude of the Range of Different Cost Values

in the probability of large losses and, thus, the upper tail of the distribution of potential losses (McNeil et al., 2005, p. 26).

While a growing number of risks leads to an increase in the calculated μ, the resulting increase of the Value-at-Risk characteristics is slightly stronger. Therefore, looking at extremal values gets more important in larger scenarios. Like shown in figure 4.6, the statistical spread increases with a growing number of risks, which means that the uncertainty – and with it the "risk" associated with the scenario – increases.

Table 4.3 lists the three probability density statistics μ, σ, and the Value-at-Risk (with α=0.9), as well as the number of different cost values on the finally resulting distribution's x-axis (#c) for six different scenarios. The only difference between each listed scenario is that one parameter is changed (i. e., arithmetically doubled), while all other parameters remain equal. The "base" scenario uses the following parameters: the number of risks R is set to 20, and the scenario consists of 1,000 components in total[2]. The cost values for each risk c_r^x are fixed to 10. We target an expected aggregated risk occurrence probability $\hat{p}_r^x$ of 0.1 in order to be able to double the probability for the sensitivity analysis. If we would continue

[2] Please note that the statistics remain the same, regardless of whether we use 1,000 services with 1,000 service-related risks or a scenario with 500 services and 500 data transfers with 500 related risks each. The statistics for both alternatives are as shown in table 4.3 for the base scenario.

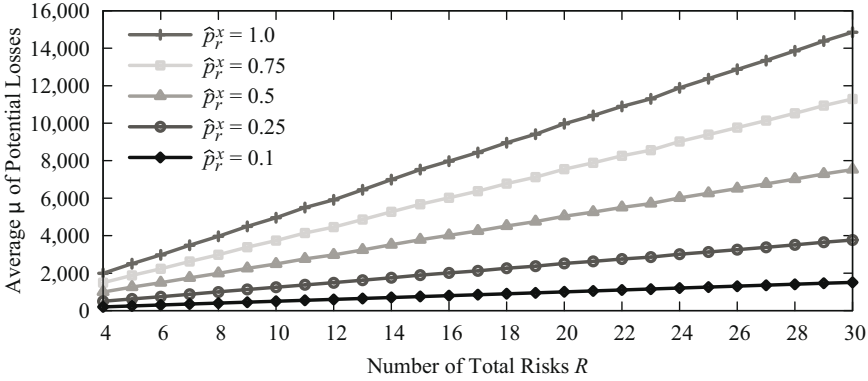


Figure 4.8 Average Potential Losses as a Function of the Aggregated Risk Occurrence Probability

using $\hat{p}_r^x = 0.5$, arithmetical doubling would lead to $\hat{p}_r^x = 1$, which means that all risks always occur, and, in consequence, there would be no statistical variance in the distribution of potential losses.

The dependence of the average potential losses on the risks' expected cost values is shown in figure 4.7. The five curves for the different magnitudes run parallel on the $\log_{10}$-axis, which can again be explained using equation (4.19). For example, a tenfold increase of the c_r^x leads to a tenfold increase of the average μ of the potential losses.

Comparison of the base scenario with the "double costs" scenario in table 4.3 shows that arithmetical doubling of the cost values leads to a doubling of all three distribution characteristics μ, σ, and the Value-at-Risk. The number of values on the x-axis (#c) remains the same for both scenarios and even the shape of the distribution does not change.

Even with a doubling of the individual cost values c_{rk}^x when dependent losses are used, all risk characteristics are exactly doubled. This means that all cost-related parameters do not change the shape of the distribution of potential losses. Instead, they only affect the x-axis, i. e., if all of the risks' expected cost values are arithmetically doubled, than the x-axis is stretched by the factor two. Likewise, if the potential losses of each risk can be reduced by one third, than all values on the x-axis will shrunk by the same factor.

The steepness of the curves is influenced by the targeted expected aggregated occurrence probability, $\hat{p}_r^x$. Figure 4.8 shows that the curve for $\hat{p}_r^x = 0.5$ (green) runs exactly between the curve for $\hat{p}_r^x = 1.0$ (red) and the x-axis. This means that

if a countermeasure can reduce all occurrence probabilities by half, the average μ of the potential losses will be reduced by 50% accordingly.

The scenario "double components (with fixed $\hat{p}_r^x$)" in table 4.3 shows that the introduced parameter $\hat{p}_r^x$ perfectly compensates the arithmetical doubling of the number of scenario components. All risk characteristics are equal to the characteristics of the "base" scenario.

The calculated individual p_{rk}^x for p_r^x=0.1 are approximately 2.107×10^{-4} for 500 components, 1.0535×10^{-4} for 1,000 components and 5.2679×10^{-5} for 2,000 components. For the scenario "double probability" with 1,000 components and p_r^x=0.2, the calculated individual p_{rk}^x are approximately 2.2312×10^{-4}.

Analogously to the simplified notation used for equations (4.11) to (4.18), it can be shown that arithmetical doubling of the number of scenario components – while fixing the p_r^x (i. e., not readjusting the occurrence probabilities to the new number of components) – leads to less than doubling of the aggregated occurrence probability $\bar{p}_x^r$. Some manipulation of equation (4.23) yields equation (4.28):

$$\bar{p} = 1 - \prod_{k \in K'} \left(1 - p'\right) \tag{4.23}$$

$$= 1 - \left(1 - p'\right)^{\mathbf{2}|K|} \tag{4.24}$$

$$= 1 - \left(1 - \left(1 - \sqrt[|K|]{1 - \hat{p}}\right)\right)^{\mathbf{2}|K|} \tag{4.25}$$

$$= 1 - \left(1 - 1 + \sqrt[|K|]{1 - \hat{p}}\right)^{\mathbf{2}|K|} \tag{4.26}$$

$$= 1 - \left(\sqrt[|K|]{1 - \hat{p}}\right)^{\mathbf{2}|K|} \tag{4.27}$$

$$= 1 - (1 - \hat{p})^{\mathbf{2}} \tag{4.28}$$

Accordingly, for $\hat{p}$=0.1 and $|K|$=1,000, an increase to $|K'|$=2,000 scenario components would lead to a calculated occurrence probability per risk of $\bar{p}$=0.19. This, in combination with equation (4.19), explains the mean value μ of 38 for the "double components (with fixed p_r^x)" scenario in table 4.3: $20 \cdot 0.19 \cdot 10 = 38$.

In conclusion, arithmetical doubling of scenario parameters has the same – or almost the same in case of the "double components (with fixed p_r^x)" scenario – effect on the mean potential losses μ. Therefore, it is important to look at the distribution of the potential losses and incorporate other characteristics, such as the standard deviation σ and the Value-at-Risk, into the decision process (McNeil et al., 2005, p. 26).

The only parameter which directly changes the number of cost values on the final distribution's x-axis (#c) is the number of risks R. For every added risk, the number of values increases and the shape of the distribution appears to be "finer". Furthermore, it could be shown that the cost-related values have a linear effect on the resulting characteristics. If all potential losses of each risk are increased by a factor, the characteristics increase by the same factor. On the contrary, if the occurrence probabilities are increased by the factor two, the σ and Value-at-Risk characteristics only increase by approximately 150%. Finally, it could be shown, that the number of scenario components (with fixed individual occurrence probabilities p_r^x) has an effect that is less than the effect of changing the occurrence probabilities.

These findings indicate that decision makers need to be aware of the fact that scenarios are more sensitive to changes in the amount of the potential losses, while changes to the occurrence probabilities or the number of risks have a less strong effect on the resulting distribution. The least strong effect is related to the number of considered components in the scenario.

Table 4.3 Sensitivity to Arithmetical Doubling of Scenario Parameters

Scenario	#c	μ	σ	VaR (α=0.9)
Base	21	20	13.416	40
Double risks	41	40	18.974	60
Double costs	21	40	26.833	80
Double probability	21	40	17.889	60
Double components (with fixed $\hat{p}_r^x$)	21	20	13.416	40
Double components (with fixed p_r^x)	21	38	17.545	60

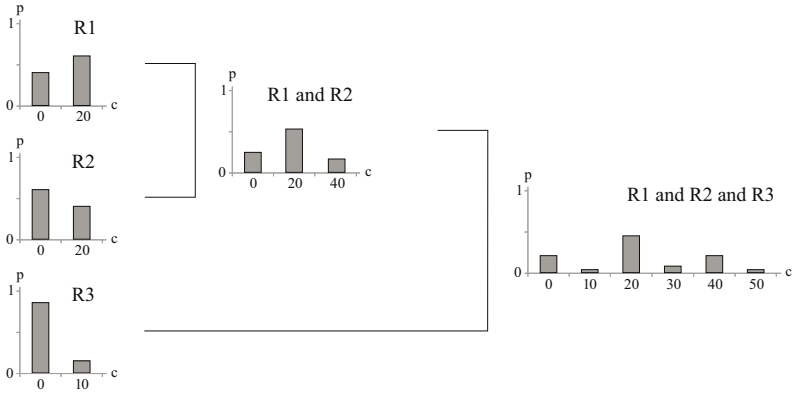


Figure 4.9 Calculation of the Joint Density Function With Rounding ($a = 10$)

4.2.3 Trade-off: Accuracy and Performance

Every user of an investment assessment model faces the trade-off between accuracy of estimation and expenditure for the elicitation of the input data.

On the one hand, a reduction of the requested accuracy can accelerate the collection of data. Experience from expert interviews conducted to evaluate the model indicates for example that the potential losses are more difficult to estimate than the occurrence probabilities which can at least always be classified on a scale from low to high. In the following, we focus on the effect of less accurate cost values. However, structurally similar considerations are also possible for the occurrence probabilities.

On the other hand, our model allows that a lower accuracy can lead to increased performance of the calculations, because of the special problem structure: The number of possible cost values on the x-axis does not grow exponentially, because more and more cost values add up to the same sum.

For instance, compare figures 4.2 and 4.9. The only difference of figure 4.9 is that all cost values on the x-axes have been rounded to the nearest multiple of 10. Figure 4.2 does not use rounding and contains potential losses of 15 for R1. As both distributions, R1 and R2, now contain the same cost value (i. e., 20), the resulting joined distribution contains one value less on its x-axis. When this joined distribution is further joined with R3, the overall discrete probability density function contains six instead of eight cost values on the x-axis.

As another example, if we draw 16 random cost values $\in \mathbb{N}$ from $[1;\ 1{,}000]$, their sum is distributed in $[16;\ 16{,}000]$ and the values in the middle of this interval are more likely. Note that this effect is much stronger for distributions where cer-

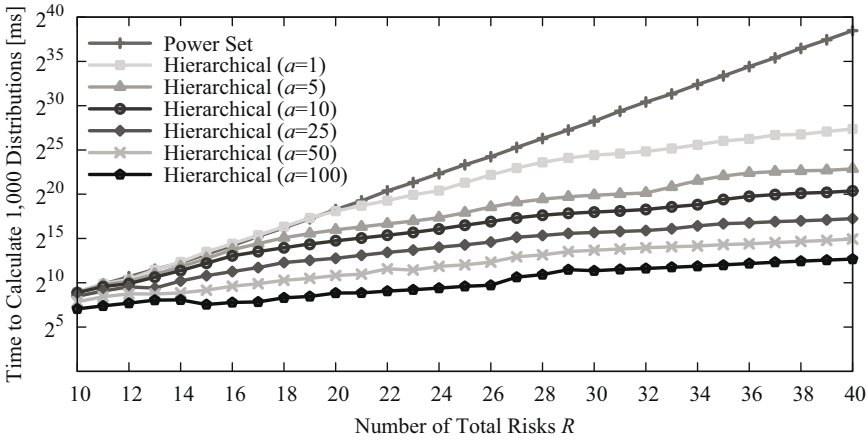


Figure 4.10 Performance of the Power Set and the new Hierarchical Approach

tain values occur more frequently than others, i. e., distributions with a relatively small variance.

Figure 4.3 shows the hierarchy for 16 risks. For 32 risks, the last calculation step would be to calculate the joint probability distribution for risks 1 to 16 and risks 17 to 32, which could both contain up to $65,536$ cost values on the x-axis. This would correspond to almost 4.3 billion ($= 65{,}536^2$) multiplications. However, because the initial costs values $\in \mathbb{N}$ were drawn from $[1;\ 1{,}000]$, there can be $16,000$ different values at most on each x-axis and the calculation would take at most 256 million ($=16{,}000^2$) multiplications. This effect gets stronger, if more risks are considered or the number of different cost values is reduced.

Therefore, an important effect of our approach is that it is possible to speed up the calculations by combining similar cost values, as this also reduces the number of values on the distributions' x-axes. The combining is done once, before the hierarchical approach starts with joining the distributions. Therefore, we introduce the rounding parameter a, which is 1 per default, and round every cost value to be a multiple of a before the joins are calculated. For example, this means that, while it is possible to calculate with costs such as 101.05, the calculations will be faster if only rounded values such as 100.0 are used. This corresponds to less accurate – and therefore cheaper – estimation of the cost values.

In order to analyze the speedup caused by the hierarchical approach and rounding the cost values, we measured the time it took to calculate 1,000 generated scenarios on one core of an AMD Opteron 8356 with 2.3 GHz. The cost values $\in \mathbb{N}$ for each risk have been drawn randomly from $[1;\ 1{,}000]$ and then rounded

Table 4.4 Speedup (for $R = 40$) Compared to Power Set and to Hierarchical Approach ($a = 1$)

	Speedup compared to Power Set	Speedup compared to Hierarchical with $a = 1$
Hierarchical ($a = 1$)	2,182	-
Hierarchical ($a = 5$)	49,594	23
Hierarchical ($a = 10$)	277,492	127
Hierarchical ($a = 25$)	2,435,834	1,116
Hierarchical ($a = 50$)	12,027,334	5,511
Hierarchical ($a = 100$)	58,065,533	26,606

according to the parameter a. Due to very long calculation times, the curve for the power set-based algorithm in figure 4.10 has been extrapolated based on one generated scenario for the cases with more than 25 total risks, as it can easily be shown, that the calculation time approximately doubles for every added risk. All other data points are based on 1,000 randomly generated scenarios.

Between 30 and 40 risks, the calculation time increases by approximately 23% for every added risk (for $a = 1$) instead of 100% for the power set-based algorithm. Table 4.4 shows the gained speedup for calculating 1,000 distributions with 40 risks.

The middle column of table 4.4 shows that the presented hierarchical approach calculates the 1,000 probability density functions for 40 risks 58 million times faster than the power set-based algorithm. The right column shows that, using the hierarchical algorithm, there is a trade-off between speed and accuracy of the calculations. If all cost values are rounded to be multiples of 100, the 1,000 calculations are done more than 26 thousand times faster compared to calculation with costs values that have not been rounded. However, even if the effect of rounding is neglected (i. e., $a = 1$) the hierarchical approach is still more than 2,000 times faster than the power set-based algorithm.

In order to analyze the inaccuracy caused by rounding the cost values, we measured the difference between the calculated distributions using the following metric: The two initial discrete probability density functions are converted into cumulative distribution functions. This is done in order to make the discrete function defined for all cost values. The resulting step functions can be visualized like shown in figure 4.11. Subsequently, we add up the areas where the two step functions differ. This absolute difference is then normalized to the relative difference (in percent) by division by the total area below the step functions. In our example in figure 4.11, the relative difference would be ((1.53+0.27+1.02+0.18) / 50) = 6%.

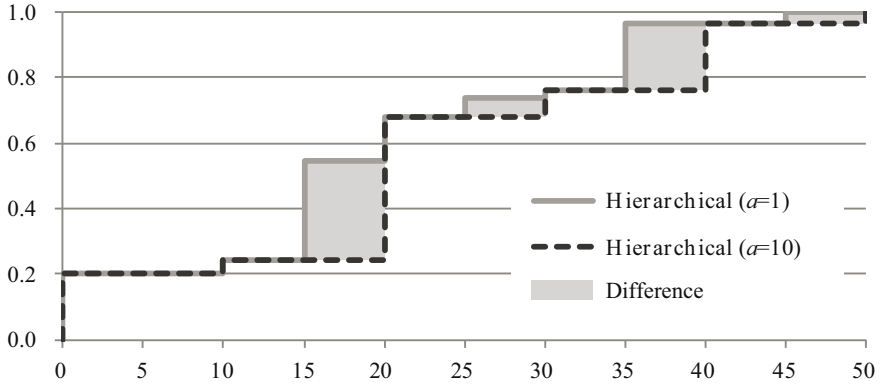


Figure 4.11 Example for the Difference Metric Between two Step Functions

Figure 4.12 shows the relative difference between 1,000 randomly generated distributions calculated based on exact and rounded ($a = 100$) cost values. Various quantiles, as well as minimum, maximum, and average for the 1,000 iterations are shown. The red line shows the maximum of measured difference and therefore fluctuates more than the other measurements. It can be clearly seen that there is a downward trend with increasing number of risks. Starting from 25 risks, 90% of the 1,000 measured differences (yellow) were already below 1%. For 40 risks, the maximum difference dropped below 2%, while the average difference (blue) was 0.3%.

This is interesting, as the differences were calculated using the highest value for the rounding parameter ($a = 100$) of our performance measurement shown in figure 4.10. As we have pointed out, rounding the cost values with that parameter provided a speedup of up to 58 million, while the average difference, i. e., the introduced inaccuracy, was below 0.3%. Especially for large scenarios, it is therefore advisable to round the values, as the distributions' differences remain small, even when high rounding parameters a are used. It might be the best approach to start with a larger a and decrease the rounding parameter a gradually when analyzing a given scenario. This allows getting quick results which are less accurate and then increase the accuracy step by step in order to refine the results.

In order to analyze whether rounding the cost values is a suitable method to manage larger scenarios that consist of many risks related to the components, we measured the size of solvable scenarios in a given time period.

Therefore, we generated scenarios including 1,000 services and 1,000 data transfers. In each iteration, we started with one risk and measured the time it took to calculate the final probability function of the potential losses on one core of an

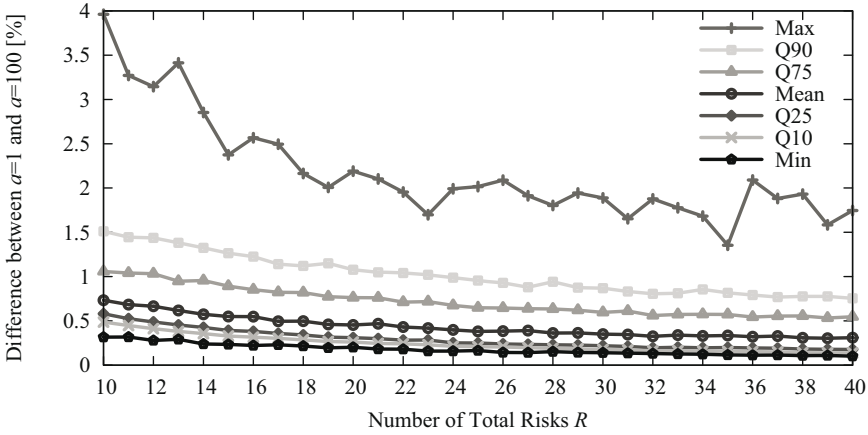


Figure 4.12 Accuracy Plot ($a = 100$)

AMD Opteron 8356 with 2.3 GHz. If the calculation's duration was less than 10 minutes, we added one more risk to the scenario and took time again. When the threshold of 10 minutes was reached, we took note of the last scenario size that was solvable. These measurements were done for various values of the rounding parameter a and the results are shown in figure 4.13 as well as table 4.5.

The visualization in figure 4.13 shows that there is a linear relationship between the rounding parameter a and the size of a scenario that can be analyzed within ten minutes. The estimated relationship is $\#\text{risks} \approx 20.5026 \cdot a + 9.1801$. The really high R^2 statistic of 0.9995 supports the hypothesis of a linear relationship. This means that rounding all parameters to the next multiple of ten would lead to $207 - 42 = 165$ more risks that can be incorporated into the risk management process. Table 4.5 lists the measured solvable size as well as the predicted solvable size of a scenario (based on the estimated relationship equation) for a given rounding parameter a.

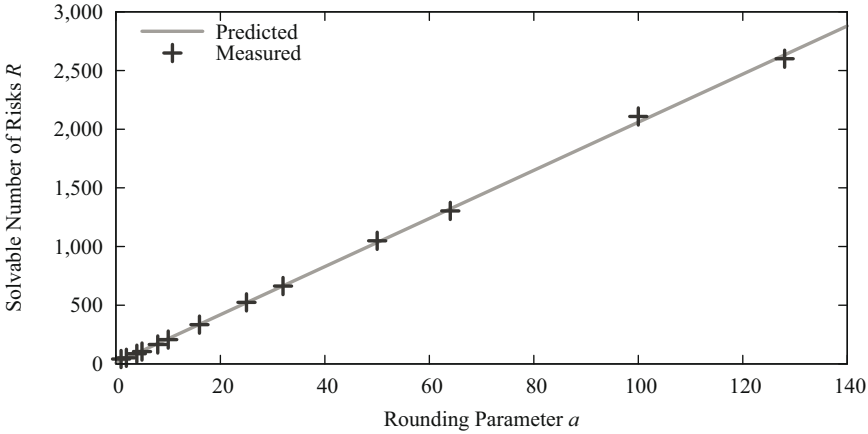


Figure 4.13 Size of Scenario Solvable per Time Depending on Rounding Parameter a

Table 4.5 Size of Scenario Solvable per Time Depending on Rounding Parameter a

a	Measured R	Predicted R
1	42	30
2	52	50
4	87	91
5	105	112
8	166	173
10	207	214
16	335	337
25	525	522
32	663	665
50	1,049	1,034
64	1,304	1,321
100	2,108	2,059
128	2,600	2,634

4.3 Model Applications

4.3.1 Dynamic Posted Pricing Service

This section contains the scenario illustration, the description of the identified major risks, and the results of our model's application[3]. The model is used to assess the aggregated risk as well as the individual cost drivers of the scenario.

4.3.1.1 Scenario Description

The scenario which we use to demonstrate our model's applicability is based on the PREMIUM-Services research project[4], more precisely on the described functionality of the Dynamic Posted Pricing (DPP) service. The project aims to develop a service which is offered to online vendors and which can be integrated into their shops. Based on various influencing factors, like a product's durability or a customer's creditworthiness, the DPP service calculates the most efficient individual price for a product that a customer shows interest in. After login, a customer visits a vendor's web page containing products. The most efficient price for some of these products can be calculated by the DPP service and is displayed to the customer as a part of an individual product page within the online shop. In the following, we describe details of the scenario whose corresponding services call graph is shown in figure 4.14.

1. The Online Shop Pricing (OSP) service determines the most efficient price using the DPP service. This price depends on different factors, like the customer's location and creditworthiness, and the demand for the product. As a consequence, the online shop transmits information about the product, e. g., past prices, as well as customer data, and the customer's Internet Protocol (IP) address, to the DPP service.
2. The DPP service tries to retrieve the customer's location and therefore sends the corresponding IP address to the Customer Location (CLo) service.
3. The CLo service returns data about the customer's location, like the names of the country, region, and city, or approximated geographical coordinates.
4. The DPP service checks the risk of credit loss using the Customer Rating (CRa) service. The transmitted data contain information about the customer, like first name, family name, and address.

[3] Compare, in the following, Ackermann and Buxmann (2010); Ackermann et al. (2013).

[4] http://premium-services.de/

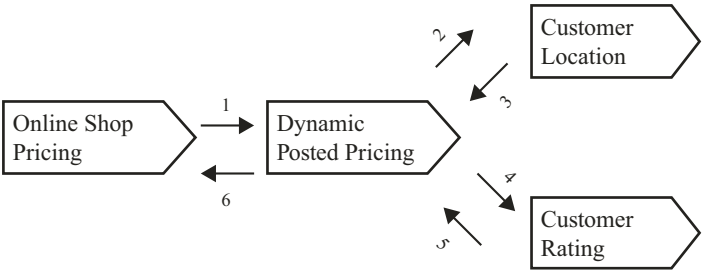


Figure 4.14 Dynamic Posted Pricing Services Scenario

5. The CRa service returns the risk of credit loss associated with the customer in form of a rating.
6. The DPP service calculates the most efficient individual price and sends it back to the online shop.

4.3.1.2 Descriptions of Identified Risks

We compare two alternative levels of security for the given scenario, i. e., security at the transport layer and security at the application layer.

For the first security level, we assume that all data are transferred encrypted using the SSL protocol. As SSL technology is the de facto standard for secure data transmissions and can easily be applied and largely reduces the risks of eavesdropping and manipulation, we do not consider less secure mechanisms. However, SSL solely provides security at the transport layer and does not ensure confidentiality or integrity at the application layer. Every service receives and processes unencrypted data and therefore service-related risks can occur with a higher probability.

The second security level provides a higher level of security by applying end-to-end security mechanisms at the application layer. Customer data, like the name, address, and IP address, are encrypted by the online shop for the CLo and CRa services and cannot be read by the DPP service. The DPP service only forwards the encrypted data to the appropriate services which are able to decrypt the information. Therefore, the DPP service does not learn the user's data.

We determined lock-in effects (R_1^S), performance problems (R_2^S), profile generation (R_3^S), and relay of information (R_4^S) as the four major service-related risks. Table 4.6 shows the model's parameter values for the different levels of security. The values which differ depending on the security level are marked bold.

Table 4.6 Parameters for Service-related Risks

	Global			OSP		DPP		CLo		CRa d_4^S=0.25	
	c	p	f	p	c	p	c	p	c	p	c
Security Level 1: SSL encryption											
R_1^S	0	-		0.0	0	**0.4**	150	**0.08**	20	**0.2**	100
R_2^S	40	-	✓	**0.08**	0	0.2	0	**0.08**	0	**0.4**	0
R_3^S	60	-	✓	0.0	0	**0.2**	0	0.08	0	0.08	0
R_4^S	170	-	✓	0.0	0	**0.2**	0	0.08	0	0.2	0
Security Level 2: SSL and end-to-end encryption											
R_1^S	0	-		0.0	0	**0.5**	150	**0.18**	20	**0.3**	100
R_2^S	40	-	✓	**0.18**	0	0.2	0	**0.18**	0	**0.5**	0
R_3^S	60	-	✓	0.0	0	**0.002**	0	0.08	0	0.08	0
R_4^S	170	-	✓	0.0	0	**0.002**	0	0.08	0	0.2	0

c: costs, p: occurrence probabilities, f: flag if risk can occur per service invocation.

1. R_1^S: The usage of external services that are not provided by multiple providers creates a vendor lock-in effect because the service consumers are not able to switch to another equivalent service, and therefore are bound to the only existing service provider (Jurison, 1995; Aubert and Rivard, 1998; Hansen, 2005; Lacity et al., 2009). If the provider stops the service, there is no fall-back solution for the consumers. The probability that lock-in effects occur is the highest for the DPP service, as no comparable services are offered on the market, while the probability for the CLo is rather low as there are alternative providers available which are able to map IP addresses to locations.
2. R_2^S: The more complex a service is, the higher is the probability that it may suffer from performance problems or may even be completely unavailable. The execution of the CRa service and the DPP service involve more processing compared to the two other services, and therefore the occurrence probabilities $p_{2;\text{DPP}}^S$ and $p_{2;\text{CRa}}^S$ are higher.
3. R_3^S: By surveying the data that are send to and received from the CLo and CRa services, it could be possible for the DPP service's provider to create detailed profiles of the online shop's customers. This confidential data could contain the customers' identities, addresses, locations, credit ratings and visited product pages. While this surveying might be possible for security level 1 (with $p_{3;\text{DPP}}^S = 0.2$), it is no longer possible if the online shop uses end-to-end encryption so

Table 4.7 Parameters for Data Transfer-related Risks

	Global			DT1		DT2		DT3		DT4		DT5		DT6	
	c	p	f	p	c	p	c	p	c	p	c	p	c	p	c
Security Level 1: SSL encryption															
R_1^T	0	0.08	✓	**1.0**	160	**1.0**	20	1.0	20	**1.0**	160	1.0	20	1.0	0
R_2^T	25	-	✓	0.0	0	0.0	0	0.0	0	0.0	0	0.08	0	0.0	0
R_3^T	30	-	✓	0.0	0	0.0	0	0.0	0	0.0	0	0.0	0	0.08	0
Security Level 2: SSL and end-to-end encryption															
R_1^T	0	0.08	✓	**0.04**	160	**0.04**	20	1.0	20	**0.04**	160	1.0	20	1.0	0
R_2^T	25	-	✓	0.0	0	0.0	0	0.0	0	0.0	0	0.08	0	0.0	0
R_3^T	30	-	✓	0.0	0	0.0	0	0.0	0	0.0	0	0.0	0	0.08	0

c: costs, p: occurrence probabilities, f: flag if risk can occur per data transfer.

that only the CLo and CRa services can decrypt and use the data. Thus, $p^S_{3;\text{DPP}} = 0.002$ for security level 2 because the DPP service in-between cannot decrypt the data.

4. R_4^S: A malicious DPP service could relay confidential customer information to third parties, resulting in high losses due to data breaches. We estimate that the loss or theft of personal information could result in the highest total costs among our identified major risks. These costs include investigating the breach, notifying customers, restoring security infrastructures as well as recovering lost business (Ponemon, 2009; Cavusoglu et al., 2004b). Like R_3^S, this risk can be largely reduced for the DPP service by using end-to-end encryption (i. e., security level 2).

Furthermore, we determined eavesdropping of customer data (R_1^T), manipulation of the credit rating (R_2^T), and manipulation of the calculated individual price (R_3^T) as the three major data transfer-related risks. The parameter values for both levels of security are shown in table 4.7.

1. R_1^T: The major data transfer-related risk is eavesdropping of customer data. Especially the invocations of the DPP or the CRa service are interesting for attackers because the transmitted data include confidential information like name and address. The occurrence probabilities for eavesdropping decrease when end-to-end encryption is used. Therefore, at security level 2, the data transfers 1, 2, and 4 are protected by two security measures: the SSL protocol and end-to-end encryption. The risk of eavesdropping is associated with the highest cost of all

data transfer-related risks because leakage of sensitive customer data might be associated with lost customers, damage to the brand and company image, legal cost and penalties as well as employee downtime (Ponemon, 2009; Cavusoglu et al., 2004b).

2. R_2^T: Via intelligent manipulation of the customers' credit ratings, it might be possible for an attacker to influence the pricing calculations in the DPP service which would result in diverging prices that are displayed to the customers. The credit rating is only part of data transfer 5 which does not use additional security at the application layer because the DPP service needs to process the data of the CRa service in order to calculate the price. Therefore, the occurrence probability $p_{2;\mathrm{DT5}}^T$ is not influenced by end-to-end encryption.
3. R_3^T: Another data transfer-related risk is the manipulation of the calculated individual prices in data transfer 6 which is also not end-to-end encrypted as both ends (i. e., the DPP and the OSP service) are directly communicating with each other. An attacker could return manipulated values to the online shop's pricing service (OSP) and thus the online shop would present wrong prices to the customer. This could result in losses for the online shop if the manipulated values are low or in lost sales because of prices which are too high for the customers. Like R_2^T, this risk cannot be mitigated or reduced by using end-to-end encryption.

In tables 4.6 and 4.7, we present our model parameters for the occurrence probabilities and costs. Our estimations are based on recent security papers, reports and surveys (e. g., Richardson, 2009; Ponemon, 2009; van Kessel, 2009; Patterson, 2002; Campbell et al., 2003; Cavusoglu et al., 2004b). Note that these estimations serve for demonstration purposes only. As we deal with a fictional online shop and new services, no historical data are available from which we could extract the parameters like, e. g., Wang et al. (2008, pp. 109–116) did.

4.3.1.3 Assessment of Aggregated Risk

In the following, we present the results of applying our model and algorithms on the described scenario. Figure 4.15 shows the costs' probability density function and the Values-at-Risk (for $\alpha = 0.9$) calculated for the two alternative levels of security. Both distribution contain 179 mappings of cost values to their occurrence probabilities, i. e., values on the x-axis of the discrete probability density function, ranging from zero, in the best case, to 980 in the worst case where all possible risks occur simultaneously. Figure 4.15 shows only those cost values smaller than 740 as the probability of larger values (up to 980) is 0.001 or smaller.

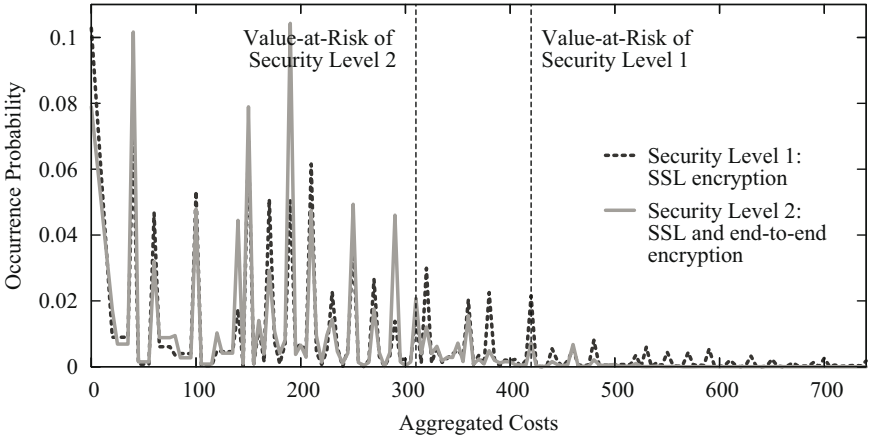


Figure 4.15 Dynamic Posted Pricing Scenario – Aggregated Costs

The distribution for security level 2 (solid red line) shows higher peaks for potential losses below 300. The first level of security's distribution (dashed blue line) shows visibly higher peaks for losses above 300, meaning that the occurrence probability for these greater losses is higher for security level 1. Risk-neutral decision makers draw their conclusions based on the expected value μ_i of the occurring costs and do not take the amount of variation within the costs into account (Gordon and Loeb, 2002). The first level of security is associated with a higher expected value of $\mu_1 \approx 201.4$. On average, in the second security level, losses of $\mu_2 \approx 168.0$ arise. The standard deviation, which may serve as a measure of the uncertainty related to an alternative, is slightly higher ($\sigma_1 \approx 158.2$) for security level 1, compared to security level 2 ($\sigma_2 \approx 111.0$). The calculated Values-at-Risk for a confidence level of 90% are also shown in figure 4.15. The second level of security has a lower Value-at-Risk of 310, while the first security level has a Value-at-Risk of 420. This means that with a probability of error of 10%, the arising losses will be equal to or lower than 310 or 420.

Decision makers who are willing to take risks or who are risk-averse can use more complex utility functions like the μ-σ-rule, which calculates the "attractiveness" or utility of an alternative based on the mean value and the distribution's standard deviation. Using the μ-σ-rule, like $-\Phi(\mu_i, \sigma_i) = -\mu_i - \lambda \cdot \sigma_i$, the utility function Φ can be adapted to a decision maker's risk preference by varying the parameter λ. For negative values of λ, the decision maker is willing to take risks, while positive values of λ represent risk-averse attitudes. Figure 4.16 shows the utility functions' lines for varying values of the parameter λ for both levels of security. Both lines intercept at $\lambda \approx -0.71$ and so two decision makers with

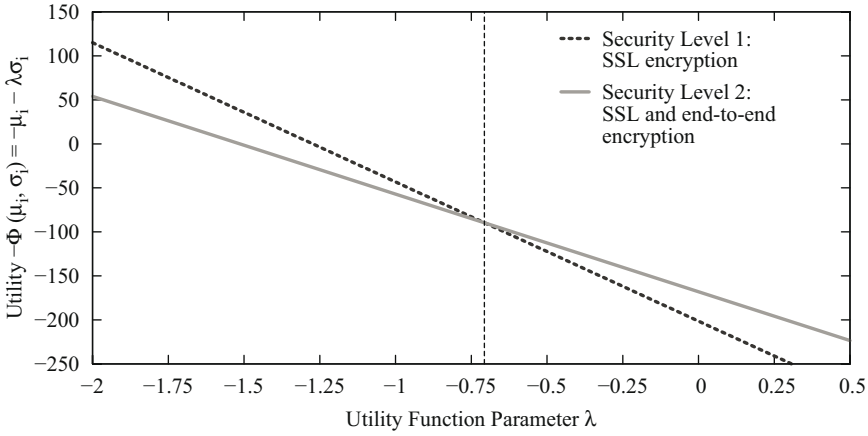


Figure 4.16 Utility Functions for the Alternative Security Levels

risk preference parameters λ below and above -0.71 would rate the two alternatives differently. For $\lambda < -0.71$, i. e., higher risk-affinity, security level 1 provides a higher utility, while for a decision maker who is less willing to take risk with $\lambda > -0.71$, security level 2 is more favorable.

Note that the implementation costs for each of the security levels have to be considered when comparing alternatives, as the difference in expected losses might not be worth the higher implementation costs. These costs can, for example, be quantified using standard methods for cost estimation of IT projects (Boehm, 1981). Assuming that the decision maker is risk-neutral and the implementation costs for both alternatives are identical, the optimal security level is to use SSL and additional end-to-end encryption (i. e., security level 2), as it largely mitigates risks, such as profile generation, as well as relay and eavesdropping of information.

4.3.1.4 Identification of Costs Drivers

As described in section 4.2.1, the proposed model can be used to identify the cost drivers of a given scenario. Cost drivers are those risks and components, such as services or data transfers, that contribute a large amount to the aggregated distribution of potential losses.

In this section, the model will be used to find the (on average) most expensive risks and the critical and most risky components for the first level of security of the DPP scenario, presented in section 4.3.1.1. This means, that we only look at

Table 4.8 Risk Contribution of the Individual Risks

Risk	#c	μ	σ	VaR (α=0.9)
R_1^S	8	**81.6**	83.8	**170**
R_2^S	2	16.2	19.6	40
R_3^S	2	16.8	26.9	60
R_4^S	2	51.7	78.2	**170**
R_1^T	12	30.4	**103.1**	0
R_2^T	2	2.0	6.8	0
R_3^T	2	2.8	9.5	0

all risks described in section 4.3.1.2, but from the perspective of security level 1, where only SSL encryption is used in order to secure the data transfers.

Table 4.8 shows that only two risks (R_1^S and R_1^T) use individual costs c_{ij}, as there the number of cost values on the x-axis (#*c*) is greater than two. The other five risks have two costs values on their x-axes: zero if the risk does not occur and the global costs if the risks occurs. Therefore, these five distributions look similar to the distributions shown at the left side of figures 4.2 and 4.9.

The sum of all μs (201.4) equals the overall distribution's expected value of the potential losses. Additionally, the sum of all squared σs (25,017.2) equals the square of the overall σ. The Values-at-Risk sum up to 440, which is more than the Value-at-Risk of the overall distribution (420) and confirms that the Value-at-Risk is not additive.

R_1^S, the risk of lock-in effects, accounts for 41% and 28% of the overall μ and σ and can therefore be considered to be the scenario's most serious risk. In order to reduce the effect of this cost driver, countermeasures, such as an alternative provider as a fallback solution or service level agreements with penalties in case of downtime, ideally monitored by a trusted third party (Osei-Bryson and Ngwenyama, 2006), could be implemented.

The next serious risks (R_4^S, R_1^T, and R_3^S) could be reduced by additional security at the application layer (Biskup, 2009). As it was shown during the presentation of the two alternative levels of security in section 4.3.1.2, SSL only provides security at the transport layer. Therefore, the protection of sensitive customer data (such as the name, address, and IP address) can be increased by applying additional end-to-end security mechanisms. If the OSP service encrypts the data in a way that only CLo and CRa can read, the potentially malicious DPP service in-between could not read and learn the data. The central DPP service would only be able to forward the encrypted data.

Table 4.9 Risk Contribution of each Service and Data Transfer

Service	#c	μ	σ	VaR (α=0.9)
OSP	8	3.2	10.9	0
DPP	15	**114.0**	**104.2**	**230**
CLo	14	23.2	50.4	60
CRa	14	35.3	57.7	100
Data Transfer	#c	μ	σ	VaR (α=0.9)
DT1	8	**12.8**	**43.4**	0
DT2	8	1.6	5.4	0
DT3	8	1.6	5.4	0
DT4	8	**12.8**	**43.4**	0
DT5	8	3.6	8.7	**20**
DT6	4	2.8	9.5	0

Although R_1^T is only responsible for 15% of the average potential losses, this data transfer alone accounts for 42% of the total variance in possible cost values. This means that it introduces a great portion of the total uncertainty.

Table 4.9 shows that the central DPP service is most critical, followed by the CRa service. Especially the DPP service accounts for a very large portion of the total potential losses, i. e., 65%. Additionally, this central service is responsible for 64% of the variance in the distribution of potential losses.

Data transfers 1 and 4 have the highest μ and σ characteristics, because they both contain sensitive customer data. In each case, with 36% and 47%, they contribute a large amount of the average losses (μ) and the total uncertainness (σ).

If we look at single cells' level, R_1^S and R_4^S are associated with the highest individual μ in combination with the central DPP service. The third highest average individual losses are caused by vendor lock-in (R_1^S) in the CRa service.

Tables 4.8 and 4.9 show that the Value-at-Risk of a discrete probability density function is equal to one of the distribution's cost values. For distributions with only two values on the x-axis, this means that the Value-at-Risk equals zero if the overall probability of the risk not to occur (calculated using 1 - equation (4.2)) is greater than the confidence level α. In our scenario, R_1^T to R_3^T, OSP, DT1 to DT4, and DT6 have an occurrence probability for no costs of 0.92 and, thus, a Value-at-Risk of zero. The Value-at-Risk is therefore a better indicator when it is used in distributions with more cost values on the x-axis, such as the overall distribution of potential losses for the whole scenario. As we have shown, the Value-at-Risk has poor aggregation properties (McNeil et al., 2005, p. 40) and is not as good as μ and σ for identifying cost drivers because it is not an additive risk measure.

4.3.2 Decision Support System Prototype

In order to practically support the IT risk management process related to Cloud Computing scenarios, a decision support system prototype was developed in PHP 5.3.

The prototype can be used during the phases of risk quantification and treatment. The application performs all calculations described in section 4.1 and provides information about the calculations' progress. Furthermore, the application is capable of identifying the cost drivers of the given scenario (see section 4.2.1) and it can visualize graphs of the calculated aggregated probability density functions of the potential losses in order to make investment decisions based on individual risk metrics.

The application – which can be used to analyze risks in Cloud Computing scenarios – is itself a SaaS application that is provided via the Internet and can be used with all modern browsers.

Due to the confidentiality of the processed information, additional requirements on security were deduced from general objectives in IT security and the ten most frequently security risks of web applications (The Open Web Application Security Project (OWASP), 2010). These requirements lead to several security-related measures: The application can only be used after successful user authentication. For this, the user's e-mail address is uniquely validated before the first use and the selected passwords must meet certain complexity requirements. Passwords are not stored in plain-text, but are salted and hashed using eight rounds of the Blowfish algorithm. Additionally, all models and parameters of scenarios stored on the server's database are encrypted with Advanced Encryption Standard (AES)-256 with a key that is derived from the user's password. Therefore, it is not possible for the provider to learn about the scenarios stored in the database. All user input is consistently validated through a combination of whitelisting and correction, on the client as well as on the server side. A web application framework is used, which contributes parameterized database access in order to prevent Structured Query Language (SQL) injections. Furthermore, the developed SaaS application requires the existence of an encrypted connection (HTTPS) for all data transfers. Cookies can be transferred via Secure flags only over SSL. Cross Site Request Forgery (CSRF) attacks as well as replay attacks are prevented by applying nonces, i. e., unique, randomly generated keys. Additionally, the SaaS application supports multitenancy, i. e., different users can be served by the same system, as within the system, a strict separation of user data is guaranteed.

At the client-side, HTML5, in conjunction with CSS, JQuery, and its extension jQueryUI are used for the visualization of the application's user interface. Figures 4.17 to 4.19 show screenshots of the prototype's actual user interface.

At the beginning of a scenario's analysis, the parameters are entered (see figure 4.17). The user enters model parameters such as names, probabilities and costs of risks, services and data transfers. After completion of the entry, the model is stored in the database.

The risk-related results of the scenario are calculated and stored in the application's database, as well. Meanwhile, the user is informed on the progress of the calculation by a progress bar. Following this, the probability density function of the occurring losses is visualized in the form of a line diagram. Interesting parts of this view can be enlarged. In addition, the expected value, standard deviation and Value-at-Risk are determined (see figure 4.18).

For all individual services, data transfers, and risks, the respective cost drivers of the scenario are identified by calculating their individual contribution to the overall expected value, standard deviation, and Value-at-Risk. These characteristics of the risk distribution are presented in form of tables, such as shown in figure 4.19.

Furthermore, the parameters of a scenario and the calculated risk distribution can be exported. In order to do so, the user chooses one of the two available data formats: JSON-Format or Microsoft Excel. The scope of the exported file depends on whether it contains calculation results. If the distribution of potential losses has been calculated, it is exported together with the model's input parameters.

In summary, the developed decision support system prototype enables decision makers to quickly quantify risks in Cloud Computing scenarios. The SaaS application can be used to efficiently aggregate the estimations for individual components to a final, combined distribution of potential losses of the whole scenario. Additionally, it helps identify the cost drivers in a given scenario.

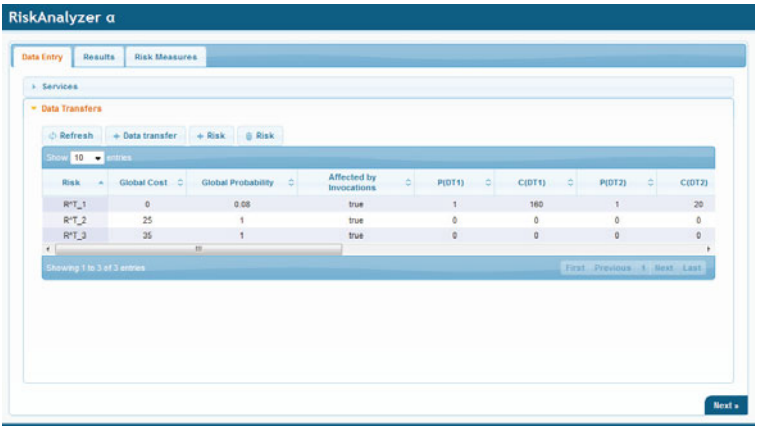


Figure 4.17 Screenshot of the Decision Support System Prototype – Parameter Entry Screen

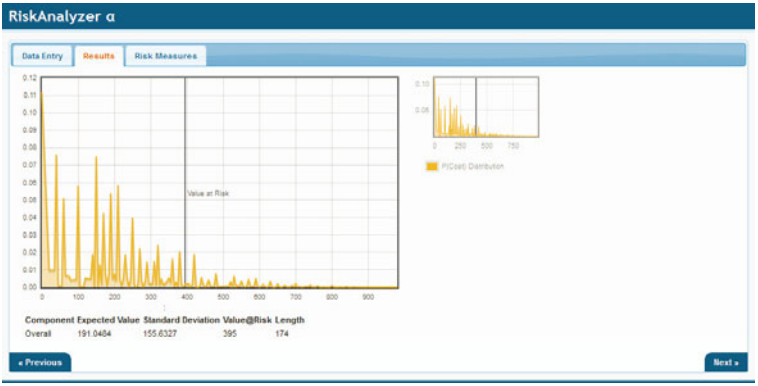


Figure 4.18 Screenshot of the Decision Support System Prototype – Results Visualization

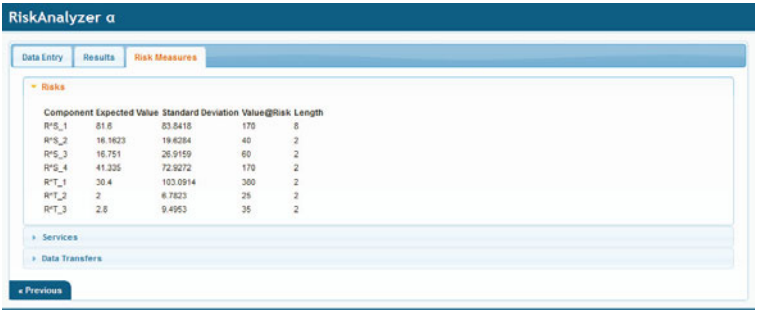


Figure 4.19 Screenshot of the Decision Support System Prototype – Cost Driver Details

Chapter 5
Recommended Actions

Based on the results of this thesis, recommended actions for Cloud Computing users and the four phases of their IT risk management process. These advises are presented in sections 5.1 to 5.4. Additionally, we provide recommended actions for providers of Cloud Computing services in section 5.5.

Table 5.1 shows a mapping of the different main sections of this thesis and their results to the four risk management phases. For example, the results of the mathematical modeling and simulation approach in chapter 4 support risk quantification and treatment after the risks have been identified with the help of the results obtained in chapter 3. As the last phase reviews the decisions made in the earlier phases (Faisst and Prokein, 2005; Prokein, 2008), all results of this thesis can be considered during these evaluations.

T. Ackermann, *IT Security Risk Management,* DOI 10.1007/978-3-658-01115-4_5,
© Springer Fachmedien Wiesbaden 2013

Table 5.1 Mapping of the Phases of the IT Risk Management Process to Research Methods and Chapters

	Scale Development				Survey		Modeling & Simulation		
	3.1: Literature Review	3.2: Q-Sort Method	3.3: Expert Interviews	3.4: Formal Model Specification	3.5: Scale Validation	3.6: Analysis of Adoption Decisions	4.1: Model Description	4.2: Simulations	4.3: Model Application
Risk Identification	✓	✓	✓	✓	✓				
Risk Quantification					✓	✓	✓	✓	✓
Risk Treatment					✓	✓	✓	✓	✓
Risk Review and Evaluation	✓	✓	✓	✓	✓	✓	✓	✓	✓

5.1 Recommended Actions for Risk Identification

The results of this thesis facilitate the IT risk management process of potential Cloud Computing users in multiple ways. Our literature review of IT security risks related to Cloud Computing (see section 3.1) resulted in a risk taxonomy consisting of 39 risks. The extended taxonomy is presented in tables 5.2 and 5.3. First, the provided list of IT security risks can be used as a checklist during the risk identification phase, as it includes all relevant risks for evaluating the performance of (alternative) Cloud Computing providers. Second, we provide characteristics of the 39 risks, so that the taxonomy can be used in combination with our proposed mathematical risk framework described in chapter 4.

In order to used our taxonomy as a checklist, the analyzed IT outsourcing scenario has to be divided into the services it is composed of (e. g., the activities or tasks of a business process), and the data transfers which connect the services. Tables 5.2 and 5.3 provide two columns next to each risk item which indicate whether or not the risk can affect services (AS) and/or data transfers (AT). For example, "Accidental data modifications at provider side" applies only to services, while "Eavesdropping communications" or "Network performance problems" affects only data transfers. This helps to identify possible risks related to the scenario. Among the initial 39 risk items identified through the literature review, 35 can be related to services and 17 can be related to data transfers. An earlier, more detailed version of the checklist containing more risks is published in Ackermann et al. (2011).

We recommend using a combination of the identification methods presented in Prokein (2008). In any case, collection methods, such as checklists or interviews with experts regarding the IT systems and IT security, should be used in order to identify as many risks as possible. These methods are mainly suitable for the identification of already known risks (Prokein, 2008, pp. 19f.). Additionally, analytical search methods, such as threat or attack trees that are created in collaboration with IT security experts, may find and anticipate future, previously unknown risks (e. g., Amoroso, 1994, pp. 15–29).

The accumulated list of identified risks (i. e., a company's result of the risk identification phase) should be compared with other lists such as our proposed IT security risks taxonomy (see tables 5.2 and 5.3) and other collections of Cloud Computing-related risks (e. g., Streitberger and Ruppel, 2009; European Network and Information Security Agency, 2009; Cloud Security Alliance, 2010).

When using Cloud Computing, it is important to pay special attention to certain risks such as "Disclosure of data by the provider" or "Supplier looking at sensitive data". As they occur on the provider-side, it is not possible to control countermeasures to protect sensitive data. Therefore, Cloud Computing users have to trust the

provider in implementing proper measures (e. g., Streitberger and Ruppel, 2009, pp. 16f.).

Additionally, detailed Service Level Agreements (SLAs) – including penalties for violating the availability, performance, and maintainability expectations – should be inspected and negotiated before the actual usage of Cloud Computing services. Especially the default SLAs offered by the majority of Cloud Computing providers should be critically scrutinized and, if necessary, be renegotiated with the provider (e. g., Patnayakuni and Seth, 2001, p. 182; Bahli and Rivard, 2005, pp. 178f.; Osei-Bryson and Ngwenyama, 2006, pp. 246f.). The SLAs have to specify the provider's legal liability in case of breach of contract and should contain all rights and obligations of the involved parties and both parties have to commit to these agreements. They should define details of the provided service in terms of measurable metrics agreed upon by all parties (Buyya et al., 2008, p. 11). However, currently used standard SLAs of large providers are often not very detailed, use ambiguous terms (Streitberger and Ruppel, 2009, p. 96) or free the Cloud Computing provider from certain responsibilities (Vaquero et al., 2009, p. 54). In addition, the SLAs should be monitored by appropriate automated systems (that are ideally run by neutral, third parties) and regular compliance checks should be conducted based on the collected data (Streitberger and Ruppel, 2009, p. 18).

Existing checklists of Cloud Computing security risks focused on risks that occur at the side of the provider. Interestingly, as a result of this thesis, we were able to identify five new security risks of Cloud Computing that are related to internal in-house systems and that could be exploited due to vulnerabilities of the browser or the used protocols and interfaces. When using Cloud Computing, there is the risk that unauthorized persons can look at or modify data on internal systems, that the availability of internal systems is limited, that users experience performance issues of internal systems, or that actions can be performed on internal systems which cannot be accounted to the initiator. The fact that these risks were not found during the literature review (see section 3.1), but were added during the expert interviews with IT security experts (see section 3.3) emphasizes the need for creative collection methods when identifying potential risks of a scenario. It is not enough to rely only on existing risk checklists alone.

5.2 Recommended Actions for Risk Quantification

As a result of this thesis, the phase of risk quantification of Cloud Computing users is supported by both, the findings of the empirical survey, as well as by the mathematical risk quantification framework.

The evaluation of risk perceptions (see sections 3.5.2 and 3.6) provides opportunities to compare the collected data to the individual assessments of security risks in the own system environment. Even though the collected risk assessments are certainly not suitable for all the individual components, decision makers should use the assessments as they serve as references and can provide guidance for own estimations.

The survey's results indicate that identity theft (e. g., Goodman and Ramer, 2007; Jensen et al., 2009; Viega, 2009), attacks against availability (e. g., Bhattacharya et al., 2003; Jensen et al., 2009; Zhang et al., 2009), and the risk that the supplier is looking at sensitive customer data stored or processed on its servers (e. g., Beulen et al., 2005; Briscoe and Marinos, 2009; Schwarz et al., 2009) are the risks that are perceived to be most serious. The descriptive statistics of the ten highest rated IT security risks related to Cloud Computing are shown in table 3.21. The descriptive sample characteristics for all 31 identified risks can be found in table A.12. The numbers used in table A.12 are mapped to the descriptions of risks in tables A.10 and A.11.

The collected data shows that risks related to confidentiality are perceived to be most serious, followed by availability and accountability risks. These three dimensions of IT security risks show highly significant effects on the perceived IT security risk as well as on the adoption intentions of (potential) users. The other three dimensions, i. e., integrity, performance, and maintainability, are also significant but were rated to be less serious by the surveyed IT executives.

In chapter 4, this thesis presents a mathematical risk quantification model which supports IT executives in analyzing risks in a given scenario. In order to do so, the scenario is divided into the constituting elements it is composed of, which makes it easier to identify and assess the individual risks related to these components. Exemplary components of a scenario can be services (provided in-house or through servers at a Cloud Computing provider's side) or data transfers in-between these services. The mathematical framework provides methods for aggregating the individual estimations back to a final, overall distribution of risks (i. e., a probability density function of the potential losses) for the whole scenario.

As we have pointed out in section 4.2.3, rounding the cost values (i. e., introducing inaccuracies) can lead to calculation times that were more than 25 thousand times faster than the calculation times without rounding. At the same time, the av-

erage difference between the calculated risk distributions, i. e., the introduced inaccuracy, was below 0.3%. Especially when larger scenarios have to be analyzed, decision makers may round the cost values, as the distributions' differences remain small, even when the values are heavily rounded. For quicker results, it might be the best approach to start with a high rounding parameter (and, thus, larger inaccuracies) and gradually decrease the rounding parameter. This improves the accuracy from step to step and iteratively refines the resulting distribution of risks.

Additionally, we were able to demonstrate a linear relationship between the rounding parameter and the size of a scenario that can be analyzed within a given time frame in section 4.2.3. This means that it is possible to anticipate a suitable degree of rounding for the cost values without having to wait too long for the results of the calculations. This could lead to an acceleration of the data collection for the cost estimations.

In addition to its suitability for risk identification, the extended IT security risk taxonomy of Cloud Computing presented in tables 5.2 and 5.3 can also be used to support decision makers in the phase of risk quantification[1]. For all risk items in the taxonomy shown in tables 5.2 and 5.3, we specify parameters that are relevant for using the identified security risks in combination with our mathematical risk model.

Tchankova (2002) distinguishes between hazards and perils. A hazard is a condition or circumstance that increases the chance of losses and their severity, while a peril is something which directly causes losses. The first column right to the number of sources for each risk (L) shows whether the risk directly involves costs or not, i. e., whether it is a hazard or a peril.

Compromised data confidentiality	peril	costs & probability
└ Disclosure of data by the provider	hazard	probability
└ Eavesdropping communications	hazard	probability
└ Insufficient user separation	hazard	probability

Figure 5.1 Exemplary relations between identified risks, as well as hazards and perils.

While it is possible to estimate occurrence probabilities for hazards and perils, it is not possible to quantify the potential losses caused by hazards as only perils cause direct costs. Thus, during the phase of risk quantification, it is important to be aware of the difference between these two types of risks. Additionally, there

[1] Compare, in the following, Ackermann et al. (2011).

are strong relationships between most of the identified risks, like shown in the structure in figure 5.1.

Furthermore, we marked all deliberate attacks (D). This is done in order to emphasize the severity of these attacks, especially when companies use recent types of IT outsourcing such as SaaS and Cloud Computing. For example, (distributed) denial of service attacks against the availability of a Cloud Computing service (e. g., Bhattacharya et al., 2003; Jensen et al., 2009; Dawoud et al., 2010) are always carried out on purpose, while limited scalability (e. g., Kern et al., 2002a; Gonçalves and Ballon, 2009; Brynjolfsson et al., 2010) is an unintended risk. In total, more than every third risk item can be a deliberate attack, i. e., done on purpose and in order to cause damage. Users should be aware of these deliberate attacks and actively implement countermeasures such as Intrusion Detection Systems (IDSs) and firewalls.

The last column of tables 5.2 and 5.3 (PI) indicates whether the number of service invocations or the number of data transfers from and to a service has to be taken into account when quantifying potential losses. Some risks, such as "Discontinuity of the service" (e. g., Currie and Seltsikas, 2001; Vitharana and Dharwadkar, 2007; Gewald and Dibbern, 2009; Schwarz et al., 2009), are related to the provider and so the number of service calls is irrelevant, while other risks, such as "Manipulation of transferred data" (e. g., Zhou et al., 2008; Minutoli et al., 2009), could occur in every single data transfer.

Additionally, a decision support system prototype has been implemented (see section 4.3.2), that itself is a SaaS application that is provided via the Internet and can be accessed with all modern browsers. The prototype can be used during the phases of risk quantification and risk treatment and performs all calculations described in section 4.1. Based on the proposed risk quantification framework, the risk estimations regarding the individual components of the scenario are automatically aggregated to the single overall risk distribution. Therefore, decision makers should use the developed decision support system prototype as it provides an easy to use graphical interface to the proposed mathematical risk quantification framework.

Table 5.2 Taxonomy of Technological IT-Outsourcing Risks and their Application Characteristics (1/2)

	1. Confidentiality Risks	#S	L	D	AS	AT	PI
1	Supplier looking at sensitive data	18			✓	✓	✓
2	Compromised data confidentially	15	✓	✓	✓	✓	✓
3	Disclosure of data by the provider	12	✓		✓	✓	✓
4	Insufficient protection against eavesdropping	7		✓	✓	✓	✓
5	Eavesdropping communications	4		✓		✓	✓
	2. Integrity Risks	**#S**	**L**	**D**	**AS**	**AT**	**PI**
1	Data manipulation at provider side	5	✓	✓	✓	✓	✓
2	Accidental modifications of transferred data	3	✓	✓		✓	✓
3	Manipulation of transferred data	3		✓		✓	✓
4	Accidental data modifications at provider side	2	✓	✓	✓		✓
	3. Availability Risks	**#S**	**L**	**D**	**AS**	**AT**	**PI**
1	Discontinuity of the service	13	✓		✓		
2	Insufficient availability and low uptime	12	✓		✓		✓
3	Unintentional downtime	9	✓		✓	✓	✓
4	Insufficient protection against downtime	7			✓	✓	✓
5	Service delivery problems	6			✓		✓
6	Loss of data access	5	✓		✓		
7	Technical issues and system failures	5			✓	✓	✓
8	Attacks against availability	4		✓	✓	✓	✓
9	Data loss at provider side	4	✓		✓		

#S: number of sources (out of the 65 final papers of the literature review) mentioning the risk, L: risk can directly lead to losses, D: risk can be a deliberate attack, AS: risk can affect services, AT: risk can affect data transfers, PI: risk can occur per invocation.

Table 5.3 Taxonomy of Technological IT-Outsourcing Risks and their Application Characteristics (2/2)

	4. Performance Risks	#S	L	D	AS	AT	PI
1	Network performance problems	24				✓	✓
2	Limited scalability	11			✓		✓
3	Deliberate underperformance	8		✓	✓		
4	Insufficient service performance	7	✓		✓	✓	✓
5	Insufficient protection against underperformance	4			✓	✓	✓
	5. Accountability Risks	**#S**	**L**	**D**	**AS**	**AT**	**PI**
1	Access without authorization	6		✓	✓		
2	Attackers generate costs	5	✓	✓	✓		✓
3	Identity theft	5		✓	✓	✓	
4	Insufficient logging of actions	3		✓	✓	✓	✓
5	Insufficient user separation	3		✓	✓		
	6. Maintainability Risks	**#S**	**L**	**D**	**AS**	**AT**	**PI**
1	Incompatible with new technologies	17	✓		✓		
2	Inflexibility regarding business change	14	✓		✓		
3	IT becomes undifferentiated commodity	8			✓		
4	Incompatible business processes	6			✓		
5	Proprietary technologies	6			✓		
6	Costly modifications are necessary	4	✓		✓		
7	Insufficient maintenance	4			✓		
8	Limited customization possibilities	3			✓		
9	Limited data import	3			✓		
10	Service does not perfectly fit	2	✓		✓		
11	Unfavorably timed updates	2	✓		✓		

#S: number of sources (out of the 65 final papers of the literature review) mentioning the risk, L: risk can directly lead to losses, D: risk can be a deliberate attack, AS: risk can affect services, AT: risk can affect data transfers, PI: risk can occur per invocation.

5.3 Recommended Actions for Risk Treatment

Risk treatment should primarily be targeted at those risks that have been quantified to be most serious (i. e., those with high occurrence probability and/or large potential losses) (Prokein, 2008, pp. 100f.). The results of our empirical survey among IT executives (see chapter 3) provide first orientations. Especially risks in the dimensions confidentiality and availability have been rated to be serious when Cloud Computing is used as a sourcing model.

Two of the ten highest rated risks (see table 3.21) are related to Cloud Computing providers that actively behave maliciously. At least when using online storage services, client-side encryption of the data, i. e., encryption before the data are uploaded to the provider's infrastructure, is suitable for protecting the data's confidentiality (Streitberger and Ruppel, 2009, p. 89). This way, confidentiality risks of some types of IaaS can almost completely be reduced. In the cases of SaaS and PaaS, client-side encryption is not possible, since the data has to be processed at the provider's side and, thus, has to be unencrypted. However, recent progress in the field of homomorphic encryption schemes (e. g., Smart and Vercauteren, 2010) enables calculations based on encrypted numbers without knowing the unencrypted values.

Other important security measures that should be implemented are intrusion detection systems (e. g., Eckert, 2006, pp. 674–678) as they might help to detect newer attacks that have not been identified during the risk identification phase based on anomalies in the patterns of sent and received data. Especially during the next IT risk management phase, i. e., risk review and evaluation, the collected application log files might help to analyze the attacks and security incidents which actually occurred.

Next to encryption and intrusion detection systems, companies should also apply all other countermeasures discussed in section 3.4.2.

The mathematical model provides the opportunity to quickly compare several alternative IT scenarios to each other from an economical point of view. These comparisons can also incorporate individual risk preferences of the decision maker, e. g., risk averse persons can identify scenarios with slightly higher expected potential losses but lower deviation of the values or a smaller long-tail of the risk distribution.

Regarding the risk preferences, it could be shown in section 4.2.1 that the risk quantification framework can very efficiently calculate risk metrics for decision makers whose individual risk utility follows a μ-σ-function. This also includes risk-neutral persons. However, this thesis provides efficient approaches and heuristics for risk aggregation for decision makers with more complex utility functions.

Our simulations show that it is still possible to evaluate scenarios with millions of individual components and thousands of risks.

Based on hundreds of thousands of simulation runs, the sensitivity analysis of the mathematical model in section 4.2.2 investigated the relationships between the parameters of modeled scenarios and the resulting overall distribution of potential losses. Regarding the individual risk preferences of decision makers, it could be shown that risk-neutral decision makers loose a lot of information by only looking at the mean value of potential losses and, therefore, neglecting the variance in the distribution of potential losses. Instead of using only the limited μ-characteristic, investment decisions should be based on the probability of large losses and, thus, the upper tail of the distribution of potential losses (McNeil et al., 2005, p. 26). The proposed risk quantification framework helps by providing very efficient methods for calculating the overall risk distribution and calculating more advanced risk metrics even for very large scenarios.

Additionally, it could be shown that scenarios are more sensitive to changes in the amount of the potential losses, while changes to the occurrence probabilities or the number of risks have a smaller effect on the resulting distribution. The least strong effect is related to the number of considered components in the scenario. Therefore, decision makers should focus on the risks with high costs, as a reduction of the potential losses has the biggest effect on the resulting distribution of risk (i. e., on the mean values as well as on the variance). The potential losses might, e. g., be reduced by using encrypted data or only transferring data that are absolutely necessary, so that potential losses due to data breaches are reduced.

The developed decision support system prototype (see section 4.3.2) can also be used to identify the cost drivers of a given scenario and, thus, provides initial evidence of potential improvement opportunities. Therefore, risk-related characteristics such as μ, σ or the Value-at-Risk are calculated based on the overall distribution of the potential losses and presented in the form of tables. Decision makers can use these numbers as the basis for making investment decisions in countermeasures against the most critical risks or in order to secure the most critical components of the scenario.

This thesis, thus, provides various contributions which support decision makers in minimizing IT security risks that can occur when Cloud Computing is used as a sourcing model.

5.4 Recommended Actions for Risk Review and Evaluation

The complete thesis serves to support the IT risk management process when Cloud Computing is used for sourcing software, platforms, or infrastructure as services. The previous sections provided recommendations for users of Cloud Computing for the phases of risk identification, quantification, and treatment. In the phase of risk review and evaluation, decision makers can analyze the completed risk management cycle retrospectively (Prokein, 2008, pp. 11f.), and check if the recommendations of this thesis were included.

Regarding the risk identification phase, it has to be verified that the attacks and security-related events which actually occurred and have been detected are consistent with the identified vulnerabilities, threats, and risks for the scenario. Additionally, if it has not been done yet, it is possible to check if all security risks obtained through the literature review and the expert interviews (see sections 3.1 and 3.3) have been considered and included in the collection of risks. Furthermore, it should be evaluated whether the risk classification was appropriate.

Decision makers have to review whether the occurred losses match the estimated occurrence probabilities and cost values of the risk quantification phase. Additionally, it is possible to check if their own estimations regarding the individual risks are comparable to the answers provided by the participating IT executives of our survey (see section 3.5). Possible deviations for the collected estimations must be justified.

Decision makers should review whether the investments in countermeasures (as a result of the risk treatment phase) had the desired effect from an ex-post point of view. In the case of this ex-post analysis, however, it must be considered that the frequency of loss events usually follows a stochastic distribution. Rather than focusing solely on the costs or, respectively, on the increased safety, it is important to invest in economically reasonable countermeasures, and thus consider the trade-off between cost and security (see section 4.1.1).

The developed decision support system prototype (see section 4.3.2) can be used to collect the risks related to individual components of a Cloud Computing scenario and to aggregate these estimations to the final, combined distribution of potential losses of the whole scenario. In order to economically treat the risks, it is possible to compare risks distributions of multiple, alternative security levels with each other.

5.5 Recommended Actions for Cloud Computing Providers

In section 3.6, we showed that the perceived IT security risk has a highly significant negative effect on the adoption decisions of potential Cloud Computing users. We even found a double negative effect, as, on the one hand, reservations against Cloud Computing (i. e., the perceived negative utility) increase when the perceived IT security risk is considered to be high. On the other hand, the perceived positive utility, i. e., the promised opportunities, such as cost advantages and switching flexibility, is also inhibited. Therefore, PITSR is an important parameter for Cloud Computing providers with which the adoption of the supplied services can be increased.

Based on the results of the conducted survey (see section 3.5), it can be seen, which risks are perceived to be more serious than others by the (potential) users of Cloud Computing services. According to the collected data, Cloud Computing providers should mainly focus on minimizing confidentiality risks and risks related to availability and accountability. Additionally to actually mitigating these risks, the measures taken should also be communicated to the users in order to build trust (Buxmann and Ackermann, 2010, p. 15).

Especially the security risk dimension "confidentiality" shows strong effects on the customers adoption decisions, followed by availability-, and accountability-related risks that are also highly significant. Performance- and maintainability-related risks also show significant negative effects on the intention to increase the level of Cloud Computing adoption, but these effects are less strong than for the already mentioned security risk dimensions.

Perceived integrity-related risks, such as deliberate manipulation of stored, transferred, or processed data, only have a small effect on the adoption decisions. Therefore, these risks should not be a primary target for trust building efforts.

Accreditation and certification of the services by an independent third-party assurance body can be used to signal the (potential) customers that a provider implements IT security measures in order to protect the users' data and intellectual property (e. g., Walsh, 2003, p. 105; Ma et al., 2005, p. 1073; Everett, 2009, pp. 5–7). The certificates should be based on reviews of technical security measures and process controls. Additionally, they should be renewed periodically as the effectiveness of implemented measures can change quickly (Goodman and Ramer, 2007, p. 818). Providers can build trust by communicating their continuous efforts to mitigate and reduce risks.

Cloud Computing providers – analogous to Cloud Computing users – can also use the mathematical risk quantification framework (see chapter 4) in order to model and compare multiple alternative security levels. The alternatives should be

weighed up and compared against each other for the purpose of making economically reasonable investments in security measures.

To elaborate on this point, there is also the possibility that Cloud Computing providers protect their IT systems in such a way that the perceived risk is minimized from the perspective of their (potential) users. In order to do so, the individual risks could be weighted with their collected average effect sizes (see tables 3.20, 3.21, and A.12). This would incorporate those risks perceived to be very serious to a greater amount when calculating the distribution of potential losses. In light of the users' perceptions, this would lead to maximum adoption of the services offered.

According to Conchar et al. (2004, p. 432), marketing strategies and actions can have a large influence on the risk perceived by the users. Therefore, Cloud Computing providers might segment their potential market according to risk profile characteristics and implement targeted trust building actions. However, some countermeasures against IT security risks – especially those perceived to be very serious – could be taken for granted by all potential customers and, thus, have to be implemented by the provider. If these essential security measures would not be offered, the customers would perceive this as a deficit and might not adopt the service.

Chapter 6
Limitations, Summary, and Prospect

6.1 Limitations and Critical Assessment

In the following, limitations of this thesis's research are presented. The quantification of risks in sections 3.5 and 3.6 is based on estimations of IT executives. The values are perceived risks instead of mathematically calculated values. Additionally, most respondents (69%) did not yet use Cloud Computing, and because of relatively low adoption rates in the market, the reported values represent anxieties rather than actual quantifications of facts and experiences. The assessment of risk incorporates both, the occurrence probability of the incident as well as its negative consequences, e. g., the potential losses. Therefore, all estimations should not be taken as fixed values. Instead, they may have to be adapted to each individual scenario.

Despite their nonsignificant loadings, three indicators from three different risk dimensions were not removed, in order to avoid violating each dimension's exhaustiveness. As all three indicators cover important aspects of their dimensions, were confirmed by expert interviews, and because analysis of Variance Inflation Factors (VIFs) showed that they are not redundant, we decided to keep them as part of the Perceived IT Security Risk (PITSR)'s content domain. However, future studies should reinvestigate these indicators and assess them in other contexts.

Theoretically, the collected data are only valid for the time that the survey took place and the external validity of the results may also be undermined by common method variance, as the data were collected from participants at the same time using the same survey. Even though various tests confirm that common method bias is not an issue, the developed PITSR scale should be cross-validated with a fresh, second set of data. This would also allow checking if and how much the assessment changes over time. Especially when the presented conceptualization is

T. Ackermann, *IT Security Risk Management,* DOI 10.1007/978-3-658-01115-4_6,
© Springer Fachmedien Wiesbaden 2013

transferred to domains other than Cloud Computing, the content validity should be reassessed.

According to Tversky and Kahneman (1973), Combs and Slovic (1979), and Sjöberg and Engelberg (2010), the availability of information is a cornerstone of heuristics for the individual assessment of risks. Therefore, a major security incident and the subsequent coverage in mass media could lead to changes in the perception of some risks which would then have to be reassessed.

In the presented risk quantification framework (see chapter 4), it is assumed that the decision maker can provide all model parameters. Therefore, all parameters have to be collected or estimated before the risk assessment is made, which is not always feasible. In particular, external services, i. e., services provided by third parties, are often used as black boxes. Consequently, it requires great effort to estimate parameters such as risk probabilities. Eventually, the occurrence probabilities for risks related to external services might be even higher than expected because of unknown sub-contractors and further (hidden) service invocations. Furthermore, the presented model assumes that all analyzed risks are uncorrelated with each other and that all risk parameters are estimated for the same time frame. This means that for every estimated probability and potential cost value, it has to be transparent whether the value was estimated, for example, per day, month, or year.

Another limitation is the fact that the costs related to the risks are modeled to be static, instead of following a distribution function. This simplification has been made in order to provide an algorithm that can calculate the probability distribution of arising costs for scenarios encompassing millions of services.

The results provided by the mathematical model are in the form of a probability density function of the potential losses. Instead of simply providing a single risk measure such as the mean value, these statistics represent the distribution of the costs. These distributions must be individually interpreted and, therefore, decision makers have to find the characteristics that best represent their own risk preferences and utility functions.

Finally, in IT security, largely due to its rapid technological improvements, attacks and security measures change quickly. Consequently, risk occurrence probabilities are dynamic and the model parameters have to be adapted from time to time. As historical data of risks and attacks grows older, it becomes difficult to make prognoses based on it. This stresses the importance of an iterative IT risk management process in which the phases of risk identification, quantification, and treatment are regularly repeated.

6.2 Summary

6.2.1 Theoretical Contributions

This research advances the understanding of IT security risks related to Cloud Computing by shedding light on the conceptual core of perceived IT security risk. To the best of our knowledge, this is the first conceptualization of perceived risk in IS research that – in line with traditional theories of risk perception – comprehensively captures the complex, multi-dimensional nature of the construct. Grounded on a broad literature review, Q-sort procedure, and extensive expert interviews, confidentiality, integrity, availability, performance, accountability, and maintainability were identified as the six sub-dimensions of perceived IT security risk of Cloud Computing. Additionally, a risk taxonomy containing 31 individual risks was created. The detailed conceptualization contributes to IT security research and allows for the transfer of theories on risk perception to the IS context. In particular, this in-depth conceptual framework of IT security risk perception advances the understanding of adoption decisions in IT outsourcing contexts. Tests of the nomological network of PITSR indicate that perceived IT security risk alone explains 28% of the companies' intentions to increase their adoption of Cloud Computing. This highly significant relationship shows that – next to perceived benefits and opportunities or the subjective norm – perceived IT security risks are one of the major factors influencing the adoption decisions of potential customers. Therefore, the presented conceptualization can be used to enhance existing theories.

This thesis also contributes a validated scale and thus a comprehensive operationalization that provides an intensively tested measurement instrument for perceived IT security risk related to Cloud Computing. The developed scale has been successfully evaluated; the validity and reliability of individual indicators, as well as at the construct level, have been intensively analyzed. Tests of nomological validity and known-groups comparison have also been conducted. The empirical results showed that PITSR captures the complex and multi-dimensional nature of the underlying latent construct better than prior traditional, simple and one-dimensional operationalizations. Therefore, researchers should use the scale as a platform for future research related to IT security risk (e. g., in the context of Technology Acceptance Model (TAM) and Theory of Reasoned Action (TRA)).

Based on the conceptualization and the results of the survey, this thesis contributes to a better understanding of the effect of IT security risks on Cloud Computing adoption decisions. The proposed theoretical model links perceived IT security risk with both positive and negative attitudinal evaluations in order to fully comprehend PITSR's impact in a broader nomological network. Covariance Structure Analysis (CSA) showed that different dimensions of IT security risk can both

increase reservations towards Cloud Computing (e. g., due to data losses and extended downtimes) and decrease the promised opportunities of Cloud Computing adoption (e. g., through cost advantages and switching flexibility) at the same time. Therefore, these dimensions may exhibit a double detrimental effect on Cloud Computing adoption.

Finally, a mathematical risk quantification model was proposed that can be used to analyze which IT security risk parameters influence the overall distribution of potential losses in Cloud Computing scenarios. A simulation-based sensitivity analysis identified the individual effects of parameters – such as occurrence probabilities, potential losses, number of risks, and number of components – and showed how the resulting overall risk characteristics change when the parameter values are reduced or increased. Knowledge of the individual effects and their relationships can help decision makers to better prioritize their strategies for risk treatment. Additionally, it is possible to more accurately anticipate how the overall risk is going to change when the scenario is changed.

6.2.2 Practical Contributions

The most important practical contribution is the empirical evidence that perceived IT security risk is one of the major factors that influence the customers' adoption decisions; this has implications for (potential) customers as well as providers of Cloud Computing.

For customers, the developed conceptualization, with its individual risks, furnishes useful suggestions on how to draw up contracts or Service Level Agreements (SLAs) with an IT outsourcing provider. Furthermore, the results can facilitate the IT risk management process of potential users during the phases of risk identification, quantification, and treatment. The provided conceptualization can serve as a checklist during risk identification, as it includes all relevant risks for evaluating the performance of (alternative) Cloud Computing providers.

In the course of risk quantification, estimations of internal security experts provide a first approximation and a reference with one's individual estimations should be compared. The developed decision support system prototype enables decision makers to quickly quantify risks in Cloud Computing scenarios. The proposed risk quantification framework helps them divide scenarios into the constituent elements, which simplifies estimating risk parameters such as potential losses and occurrence probabilities for individual components. The mathematical model solves the problem of efficiently aggregating individual estimations to the final, combined distribution of potential losses of the whole scenario.

Furthermore, the decision support system prototype can be used to compare alternative security scenarios. Therefore, it provides a sound basis for risk treatment, as different countermeasures can be modeled and tested against each other. Based on individual risk preferences and utility functions, decision makers can chose the most economically reasonable combination.

Additionally, the developed prototype helps decision makers identify the cost drivers in a given scenario, as it reports the individual fraction of the potential losses that is contributed by each single risk or scenario component. Thus, it is possible to analyze which components of the information system (e. g., services and data transfers) induce the highest proportion of risk and whose removal or exchange leads to the greatest reduction of potential losses during the phase of IT risk treatment.

The highly significant relation between perceived risk and the adoption intention is especially relevant, since the perceived risk can differ from the actual level of risk. This misjudgment of risk can lead to wrong or harmful decisions, like the extreme example of road kills after September 11 dramatically illustrates (Gigerenzer, 2004). Therefore, for Cloud Computing providers, there is huge potential in correcting these misjudgments. The quantification of users' individual risk perceptions can provide the basis for targeted efforts to manage these perceptions. This could be done by implementing concrete countermeasures and by well-directed communication efforts in order to build trust. The in-depth conceptualization of PITSR allows for a better understanding of the context-sensitive underlying dimensions of perceived risk, which is important, because these dimensions have to be treated differently.

6.2.3 Conclusion

Based on established guidelines, a systematic five-step process, involving a variety of methods, was used in order to develop, refine, and evaluate the conceptualization and measurement of the perceived IT security risk. Starting with an extensive literature review of 149 papers to build the initial pool of IT security risks relevant to Cloud Computing, the Q-sort method as well as interviews with 24 IT security experts were conducted in order to refine and evaluate the clustering of individual risks to six risk dimensions. The developed measurement scale for the presented construct was comprehensively validated through successful tests of nomological validity and known-groups comparison. Additionally, it was shown that the scale better captures the complex, multi-dimensional structure of the underlying latent construct than previously-used aggregated, higher-level operationalizations. Therefore, it is hoped that the conceptualization and operationalization will en-

courage future research that examines perceived IT security risk within different theoretical models and contexts, helping to provide a better understanding of user behavior.

To the best of our knowledge, this is the first study at the interface between Cloud Computing and IT security that comprehensively examines the form and nature of PITSR and its impact on IT executives' Cloud Computing assessments and adoption intentions. Tests of the construct's nomological network indicate a highly significant relationship and show that – next to perceived benefits and opportunities or the subjective norm – perceived IT security risks are an important factor that influences the adoption decisions of potential customers.

This thesis is also the first attempt to propose a theoretical model that links perceived IT security risk with both positive and negative attitudinal evaluations in order to fully comprehend its impact in a broader nomological network. The proposed model exhibited good psychometric properties and explained significant amounts of the variance of all endogenous variables. This study, thus, firmly established the multi-dimensional nature of PITSR as an important construct that influences IT executives in their decision-making process (i. e., in their trade-off between positive and negative attitudes and their subsequent adoption intentions) and provided a strong empirical basis for deeper investigations into more complex effect mechanisms triggered by perceived IT security risk.

This thesis presented a risk quantification framework that can be used to quantify the risks occurring in information systems composed of services and data transfers. It was demonstrated that it is possible to evaluate security levels and to make proper investment choices using individual risk preferences based on mathematically calculated probability density functions. By deriving metrics such as the expected value of costs or the Value-at-Risk from the distribution of potential losses, the attractiveness of investment choices can be measured and compared. Building on that, decision makers can choose an optimal security level, i. e., the most economically reasonable combination of security measures.

Simulations showed that inaccuracies in parameter estimation have a relatively small effect on calculated results, especially for large scenarios. By pre-processing and rounding the model's parameters before the calculation of joint probability density functions begins, it is possible to achieve huge speedups without sacrificing much accuracy. Unlike previous approaches, which do not support decision makers in aggregating the risks of multiple components of Cloud Computing scenarios, the mathematical model can handle realistic, larger information systems with many interconnected components and risks.

Additionally, it is possible to analyze which components of the system (e. g., services or data transfers) induce the highest proportion of risk and whose removal or exchange leads to the greatest reduction in potential losses. Based on analysis of how the model responds to changes in parameters, this thesis proved that if

appropriate risk measures are taken for the assessment of risk drivers, it is possible to show how the risk is concentrated in each individual risk, as a fraction of the overall risk.

Finally, an existing real-life e-commerce pricing system was used to demonstrate how the model can be applied in order to quantify the risks occurring in this scenario and to compare two alternative levels of security.

6.3 Recommendations for Future Work

Regarding the literature review described in section 3.1, further work needs to be done in order to extend the support of risk management to the third phase, i. e., risk treatment, by showing which countermeasures allow for the reduction of specific risks. As part of the literature review, countermeasures were collected and grouped into categories such as performance management, business continuity, logging and non-repudiation, or trust and reputation establishment. More information on the cause-and-effect chains between the identified risks and the connections to existing countermeasures would allow for the identification of which risks can be caused by other risks, as well as which countermeasures protect against which risks. The associated graphs can be used in the phase of risk treatment. This information could be particularly useful in the context of IT risk management decision support systems.

There are several avenues for further research regarding the conceptualization and operationalization of PITSR. On the conceptual level, the process of forming users' risk perceptions should be further investigated. Risk controversies are a common issue and could lead to wrong decisions, as seen in the initial example of the increase in traffic fatalities during the months following September 11 (Gigerenzer, 2004). As media coverage of single IT security incident can have an effect on the perception of all IT security risks, an event study on the basis of experimentation could be used to better understand the formation process of risk perceptions. This thesis serves as a first step towards research on risk controversies related to IT security in the context of Cloud Computing. By comparing the collected perceived risks with actual risks, it might be possible to analyze the cause and effect relationships of misjudged risks. Therefore, the expert interviews with IT security experts described in section 3.3 should be extended. A number of possible future studies using the same domain and set of questions are apparent. More information on the risk quantifications of IT security experts would allow for the establishment of more objective ratings of the collected risks that could serve as reference values.

A future study investigating the risks seen from the Cloud Computing providers' and from the IT security experts' views would also be very interesting. The data could be used to compare a) clients' and providers' perceived risks, as well as b) the users' perceived risks and the estimations of experts, which are supposed to be neutral.

The PITSR scale and operationalization developed throughout chapter 3 should be cross-validated on a fresh, second set of data (MacKenzie et al., 2011, pp. 324f.). As the new samples should be obtained from another population to which the PITSR scale is expected to apply, this step could be combined with

collecting risk assessments from Cloud Computing providers and IT security experts. These future studies could also help other researchers reinvestigate the three problematic indicators (see section 3.5.2.6) and assess them in other contexts.

Hopefully, this thesis will serve as a springboard for future research studies and aid Cloud Computing providers in better addressing their (potential) clients' IT security risk perceptions. To the extent that researchers may be able to transfer (parts of) the scale to other IT security risk domains, PITSR may also serve as a validated baseline measure that makes it much easier to compare and consolidate findings across studies and contexts. Therefore, it is hoped that the conceptualization and operationalization will encourage future research to examine perceived IT security risk within different theoretical models and contexts, providing a better understanding of user behaviors.

Regarding the risk quantification framework described in chapter 4, further research is needed in order to determine how the scenario's probability and cost parameters can be automatically extracted based on a given business process (e. g., in the Business Process Execution Language (BPEL) format) or based on historical data sets. For example, log files of intrusion detection systems could help decision makers estimate occurrence probabilities for common attacks. Wang et al. (2008, pp. 109–116) already demonstrated how parameters, such as occurrence probabilities for IT security risks, can be extracted based on data from a host-based activity monitoring system. However, detection and quantification of IT security-related anomalies is in its early stages and, thus, the results should be scrutinized by IT security experts.

Furthermore, it would be interesting to analyze how different countermeasures and IT security technologies collaborate with each other. There might be interaction effects between security measures that are not considered in the mathematical risk model.

The decision support system prototype presented in section 4.3.2 could be extended by integrating a recommendation systems that, based on the identified risks, suggests adequate countermeasures. This would help decision makers secure their Cloud Computing scenarios.

Finally, the proposed risk quantification framework is only a first step, and offers various avenues for further research that might extend the presented mathematical model. In addition to extending the model as suggested above, future research could, and should, assess the problem of optimal security investments from a macroeconomic perspective. In contrast to evaluating risks, such as Stuxnet and Flame, at an organizational level, it might be worth considering the total effects and potential losses for the state and society.

Appendix

A.1 Sources for the Literature Review

This is the list of all 65 sources considered in the literature review presented in section 3.1:

1. Altinkemer, Kernel; Chaturvedi, Alok; and Gulati, Rakesh. Information systems outsourcing: Issues and evidence. *International Journal of Information Management*, 14 (4), pp. 252–268, 1994.
2. Aron, Ravi; Clemons, Eric K.; and Reddi, Sashi. Just Right Outsourcing: Understanding and Managing Risk. *Journal of Management Information Systems*, 22 (2), pp. 37–55, 2005.
3. Bahli, Bouchaib and Rivard, Suzanne. The information technology outsourcing risk: a transaction cost and agency theory-based perspective. *Journal of Information Technology*, 18 (3), pp. 211–221, 2003.
4. Bahli, Bouchaib and Rivard, Suzanne. Validating measures of information technology outsourcing risk factors. *Omega*, 33 (2), pp. 175–187, 2005.
5. Baldwin, Lynne P.; Irani, Zahir; and Love, Peter E. D. Outsourcing information systems: drawing lessons from a banking case study. *European Journal of Information Systems*, 10 (1), pp. 15–24, 2001.
6. Benefield, Robert. Agile Deployment: Lean Service Management and Deployment Strategies for the SaaS Enterprise. In *42nd Hawaii International Conference on System Sciences (HICSS)*, pp. 1–5, 2009.
7. Beulen, Erik; Fenema, Paul Van; and Currie, Wendy. From Application Outsourcing to Infrastructure Management: Extending the Offshore Outsourcing Service Portfolio. *European Management Journal*, 23 (2), pp. 133–144, 2005.
8. Beybutov, E. Managing of information security with outsource service provider. In *International Siberian Conference on Control and Communications (SIBCON)*, pp. 62–66, 2009.
9. Bhattacharya, Somnath; Behara, Ravi S.; and Gundersen, David E. Business risk perspectives on information systems outsourcing. *International Journal of Accounting Information Systems*, 4 (1), pp. 75–93, 2003.
10. Briscoe, Gerard and Marinos, Alexandros. Digital ecosystems in the clouds: Towards community cloud computing. In *3rd IEEE International Conference on Digital Ecosystems and Technologies (DEST)*, pp. 103–108, 2009.
11. Brynjolfsson, Erik; Hofmann, Paul; and Jordan, John. Cloud computing and electricity: beyond the utility model. *Communications of the ACM*, 53 (5), pp. 32–34, 2010.
12. Chou, David C. and Chou, Amy Y. Information systems outsourcing life cycle and risks analysis. *Computer Standards & Interfaces*, 31 (5, Sp. Iss. SI), pp. 1036–1043, 2009.
13. Currie, Wendy L. A knowledge-based risk assessment framework for evaluating web-enabled application outsourcing projects. *International Journal of Project Management*, 21 (3), pp. 207–217, 2003.
14. Currie, Wendy L. and Seltsikas, Philip. Delivering Business Critical Information Systems Though Application Service Providers: The Need for a Market Segmentation Strategy. *International Journal of Innovation Management*, 5 (3), pp. 323–349, 2001a.
15. Currie, Wendy L. and Seltsikas, Philip. Exploring the supply-side of IT outsourcing: evaluating the emerging role of application service providers. *European Journal of Information Systems*, 10 (3), pp. 123–134, 2001b.
16. Currie, Wendy L.; Michell, Vaughan; and Abanishe, Oluwakemi. Knowledge process outsourcing in financial services: The vendor perspective. *European Management Journal*, 26 (2), pp. 94–104, 2008.

T. Ackermann, *IT Security Risk Management,* DOI 10.1007/978-3-658-01115-4,
© Springer Fachmedien Wiesbaden 2013

17. Dawoud, Wesam; Takouna, Ibrahim; and Meinel, Christoph. Infrastructure as a service security: Challenges and solutions. In *7th International Conference on Informatics and Systems (INFOS)*, pp. 1–8, 2010.
18. de Chaves, Shirlei Aparecida; Westphall, Carlos Becker; and Lamin, Flavio Rodrigo. SLA Perspective in Security Management for Cloud Computing. In *6th International Conference on Networking and Services (ICNS)*, pp. 212–217, 2010.
19. Dikaiakos, Marios D.; Katsaros, Dimitrios; Mehra, Pankaj; Pallis, George; and Vakali, Athena. Cloud Computing: Distributed Internet Computing for IT and Scientific Research. *IEEE Internet Computing*, 13 (5), pp. 10–13, 2009.
20. Everett, Catherine. Cloud computing - A question of trust. *Computer Fraud & Security*, 2009 (6), pp. 5–7, 2009.
21. Fowler, Alan and Jeffs, Ben. Examining Information Systems Outsourcing: a Case Study from the United Kingdom. *Journal of Information Technology (Routledge, Ltd.)*, 13 (2), pp. 111–126, 1998.
22. Gewald, Heiko and Dibbern, Jens. Risks and benefits of business process outsourcing: A study of transaction services in the German banking industry. *Information & Management*, 46 (4), pp. 249–257, 2009.
23. Gonçalves, Vânia and Ballon, Pieter. An exploratory analysis of Software as a Service and Platform as a Service models for mobile operators. In *13th International Conference on Intelligence in Next Generation Networks (ICIN)*, pp. 1–4, 2009.
24. Goodman, Seymour E. and Ramer, Rob. Global Sourcing of IT Services and Information Security: Prudence Before Playing. *Communications of AIS*, 2007 (20), pp. 812–823, 2007.
25. Grabarnik, Genady; Ludwig, Heiko; and Shwartz, Larisa. Dynamic management of outsourced service processes QoS in a service provider - service supplier environment. In *3rd IEEE/IFIP International Workshop on Business-driven IT Management (BDIM)*, pp. 81–88, 2008.
26. Greengard, Samuel. Cloud Computing and Developing Nations. *Communications of the ACM*, 53 (5), pp. 18–20, 2010.
27. Guah, Matthew W. and Currie, Wendy L. Logicality of ASP in healthcare: the NHS case study. In *37th Annual Hawaii International Conference on System Sciences (HICSS)*, pp. 1–10, 2004.
28. Gulla, Umesh and Gupta, M. P. Deciding Information Systems (IS) Outsourcing: A Multi-Criteria Hierarchical Approach. *Vikalpa: The Journal for Decision Makers*, 34 (2), pp. 25–40, 2009.
29. Hao, Jingjing. IT outsourcing risk assessment for Chinese enterprises based on service sciences and factor analysis. In *IEEE International Conference on Grey Systems and Intelligent Services (GSIS)*, pp. 1755–1758, 2009.
30. Itani, Wassim; Kayssi, Ayman; and Chehab, Ali. Privacy as a Service: Privacy-Aware Data Storage and Processing in Cloud Computing Architectures. In *8th IEEE International Conference on Dependable, Autonomic and Secure Computing (DASC)*, pp. 711–716, 2009.
31. Jayatilaka, Bandula; Schwarz, Andrew; and Hirschheim, Rudy. Determinants of ASP choice: an integrated perspective. *European Journal of Information Systems*, 12 (3), pp. 210–224, 2003.
32. Jensen, Meiko; Schwenk, Jörg; Gruschka, Nils; and Iacono, Luigi Lo. On Technical Security Issues in Cloud Computing. In *IEEE International Conference on Cloud Computing (CLOUD)*, pp. 109–116, 2009.
33. Kaufman, Lori M. Data Security in the World of Cloud Computing. *IEEE Security Privacy*, 7 (4), pp. 61–64, 2009.

34. Kern, Thomas; Kreijger, Jeroen; and Willcocks, Leslie. Exploring ASP as sourcing strategy: theoretical perspectives, propositions for practice. *The Journal of Strategic Information Systems*, 11 (2), pp. 153–177, 2002.
35. Kumar, Sameer; Aquino, Edgardo C.; and Anderson, Elizabeth. Application of a Process Methodology and a Strategic Decision Model for Business Process Outsourcing. *Information Knowledge Systems Management*, 6 (4), pp. 323–342, 2007.
36. Lu, Yonghe and Sun, Bing. The Fitness Evaluation Model of SAAS for Enterprise Information System. In *IEEE International Conference on e-Business Engineering (ICEBE)*, pp. 507–511, 2009.
37. Ma, Qingxiong; Pearson, J. Michael; and Tadisina, Suresh. An exploratory study into factors of service quality for application service providers. *Information & Management*, 42 (8), pp. 1067–1080, 2005.
38. Martinsons, Maris G. Outsourcing information systems: A strategic partnership with risks. *Long Range Planning*, 26 (3), pp. 18–25, 1993.
39. Minutoli, Giuseppe; Fazio, Maria; Paone, Maurizio; and Puliafito, Antonio. Virtual business networks with Cloud Computing and virtual machines. In *International Conference on Ultra Modern Telecommunications Workshops (ICUMT)*, pp. 1–6, 2009.
40. Mowbray, Miranda and Pearson, Siani. A client-based privacy manager for cloud computing. In *4th International ICST Conference on COMmunication System softWAre and middlewaRE (COMSWARE)*, ACM, New York, NY, USA, pp. 1–8, 2009.
41. Nakatsu, Robbie T. and Iacovou, Charalambos L. A comparative study of important risk factors involved in offshore and domestic outsourcing of software development projects: A two-panel Delphi study. *Information & Management*, 46 (1), pp. 57–68, 2009.
42. Ngwenyama, Ojelanki K. and Bryson, Noel. Making the information systems outsourcing decision: A transaction cost approach to analyzing outsourcing decision problems. *European Journal of Operational Research*, 115 (2), pp. 351–367, 1999.
43. Oh, Wonseok; Gallivan, Michael J.; and Kim, Joung W. The Market's Perception of the Transactional Risks of Information Technology Outsourcing Announcements. *Journal of Management Information Systems*, 22 (4), pp. 271–303, 2006.
44. Osei-Bryson, Kweku-Muata and Ngwenyama, Ojelanki K. Managing risks in information systems outsourcing: An approach to analyzing outsourcing risks and structuring incentive contracts. *European Journal of Operational Research*, 174 (1), pp. 245–264, 2006.
45. Patnayakuni, Ravi and Seth, Nainika. Why license when you can rent? Risks and rewards of the application service provider model. In *ACM SIGCPR Conference on Computer Personnel Research (SIGCPR)*, ACM, New York, NY, USA, pp. 182–188, 2001.
46. Qiang, Zhang and Dong, Cui. Enhance the User Data Privacy for SAAS by Separation of Data. In *International Conference on Information Management, Innovation Management and Industrial Engineering*, vol 3, pp. 130–132, 2009.
47. Safizadeh, M. Hossein; Field, Joy M.; and Ritzman, Larry P. Sourcing practices and boundaries of the firm in the financial services industry. *Strategic Management Journal*, 29 (1), pp. 79–91, 2008.
48. Schwarz, Andrew; Jayatilaka, Bandula; Hirschheim, Rudy; and Goles, Tim. A Conjoint Approach to Understanding IT Application Services Outsourcing. *Journal of the AIS*, 10 (10), pp. 748–781, 2009.
49. Viega, John. Cloud Computing and the Common Man. *Computer*, 42 (8), pp. 106–108, 2009.
50. Vitharana, Padmal and Dharwadkar, Ravi. Information Systems Outsourcing: Linking Transaction Cost and Institutional Theories. *Communications of the AIS*, 2007 (20), pp. 346–370, 2007.
51. Walsh, Kenneth R. Analyzing the Application ASP Concept: Technologies, Economies, and Strategies. *Communications of the ACM*, 46 (8), pp. 103–107, 2003.

52. Wang, Cong; Wang, Qian; Ren, Kui; and Lou, Wenjing. Ensuring data storage security in Cloud Computing. In *17th International Workshop on Quality of Service (IWQoS)*, pp. 1–9, 2009a.
53. Wang, Cong; Wang, Qian; Ren, Kui; and Lou, Wenjing. Privacy-Preserving Public Auditing for Data Storage Security in Cloud Computing. In *29th IEEE International Conference on Computer Communications (INFOCOM)*, pp. 1–9, 2010.
54. Wang, Hui. Privacy-Preserving Data Sharing in Cloud Computing. *Journal of Computer Science and Technology*, 25 (3), pp. 401–414, 2010.
55. Wang, Jian; Zhao, Yan; Jiang, Shuo; and Le, Jiajin. Providing privacy preserving in cloud computing. In *International Conference on Test and Measurement (ICTM)*, vol 2, pp. 213–216, 2009b.
56. Willcocks, Leslie P. and Lacity, Mary C. IT Outsourcing in Insurance Services: Risk, Creative Contracting and Business Advantage. *Information Systems Journal*, 9 (3), pp. 163–180, 1999.
57. Xiong, Li; Chitti, Subramanyam; and Liu, Ling. Preserving data privacy in outsourcing data aggregation services. *ACM Transactions on Internet Technology*, 7 (3), Article 17, 2007.
58. Xu, Jing; Jinglei, Tang; Dongjian, He; and Yang, Zhang. Security Scheme for Sensitive Data in Management-Type SaaS. In *International Conference on Information Management, Innovation Management and Industrial Engineering*, vol 4, pp. 47–50, 2009.
59. Yalaho, Anicet and Nahar, Nazmun. Risk management in offshore outsourcing of software production using the ICT-supported unified process model: A cross-case study. In *Portland International Conference on Management of Engineering Technology (PICMET)*, pp. 1721–1748, 2008.
60. Yildiz, Mehmet; Abawajy, Jemal; Ercan, Tuncay; and Bernoth, Andrew. A Layered Security Approach for Cloud Computing Infrastructure. In *10th International Symposium on Pervasive Systems, Algorithms, and Networks (ISPAN)*, pp. 763–767, 2009.
61. Young, Peter C. and Hood, John. Risk and the Outsourcing of Risk Management Services: The Case of Claims Management. *Public Budgeting & Finance*, 23 (3), pp. 109–119, 2003.
62. Yu, Shucheng; Wang, Cong; Ren, Kui; and Lou, Wenjing. Achieving Secure, Scalable, and Fine-grained Data Access Control in Cloud Computing. In *29th IEEE International Conference on Computer Communications (INFOCOM)*, pp. 1–9, 2010.
63. Zhang, Xinwen; Schiffman, Joshua; Gibbs, Simon; Kunjithapatham, Anugeetha; and Jeong, Sangoh. Securing elastic applications on mobile devices for cloud computing. In *ACM workshop on Cloud Computing Security (CCSW)*, ACM, New York, NY, USA, pp. 127–134, 2009.
64. Zhang, Yue and Shi, Xiaojun. Offshore Software Outsourcing Risk Evaluation: An Experimental Approach Base on Linear Mixed Model. In *6th International Conference on Fuzzy Systems and Knowledge Discovery (FSKD)*, vol 1, pp. 505–509, 2009.
65. Zhou, Linzhen; Liu, Defang; and Wang, Bin. Research on ASP-Based Information Security System. In *International Symposium on Computer Science and Computational Technology (ISCSCT)*, vol 2, pp. 746–749, 2008.

A.2 Sources for each Risk Item

Table A.1 Sources for each Risk Item (1/2)

	1. Confidentiality Risks	#S	Sources
1	Supplier looking at sensitive data	18	[6], [7], [10], [19], [26], [30], [32], [33], [40], [41], [48], [52], [53], [54], [55], [57], [60], [63]
2	Compromised data confidentially	15	[1], [17], [32], [37], [39], [40], [45], [48], [52], [58], [60], [61], [62], [63]
3	Disclosure of data by the provider	12	[17], [30], [33], [36], [46], [49], [51], [52], [54], [55], [65]
4	Insufficient protection against eavesdropping	7	[17], [18], [38], [41], [48], [49], [51]
5	Eavesdropping communications	4	[17], [32], [49], [63]

	2. Integrity Risks	#S	Sources
1	Data manipulation at provider side	5	[17], [32], [52], [53], [54]
2	Accidental modifications of transferred data	3	[36], [54], [65]
3	Manipulation of transferred data	3	[39], [54], [65]
4	Accidental data modifications at provider side	2	[36], [65]

	3. Availability Risks	#S	Sources
1	Discontinuity of the service	13	[2], [4], [8], [13], [14], [18], [22], [34], [36], [41], [48], [50], [60]
2	Insufficient availability and low uptime	12	[6], [10], [15], [16], [25], [31], [34], [38], [39], [51], [54], [59]
3	Unintentional downtime	9	[2], [6], [7], [27], [48], [51], [54], [60], [61]
4	Insufficient protection against downtime	7	[17], [18], [34], [41], [48], [51], [63]
5	Service delivery problems	6	[4], [13], [14], [17], [22], [38]
6	Loss of data access	5	[23], [48], [49], [53], [54]
7	Technical issues and system failures	5	[6], [7], [27], [51], [60]
8	Attacks against availability	4	[9], [17], [32], [63]
9	Data loss at provider side	4	[18], [24], [36], [65]

Table A.2 Sources for each Risk Item (2/2)

	4. Performance Risks	#S	Sources
1	Network performance problems	24	[5], [7], [8], [9], [10], [11], [13], [15], [19], [23], [25], [26], [27], [34], [36], [37], [38], [39], [45], [48], [51], [60], [63], [64]
2	Limited scalability	11	[6], [9], [10], [11], [15], [16], [21], [23], [34], [39], [62]
3	Deliberate underperformance	8	[2], [13], [22], [41], [42], [43], [44], [48]
4	Insufficient service performance	7	[8], [11], [22], [34], [42], [47], [51]
5	Insufficient protection against underperformance	4	[17], [34], [51], [63]

	5. Accountability Risks	#S	Sources
1	Access without authorization	6	[18], [30], [38], [40], [46], [49]
2	Attackers generate costs	5	[10], [18], [32], [60], [63]
3	Identity theft	5	[9], [24], [32], [49], [52]
4	Insufficient logging of actions	3	[10], [18], [60]
5	Insufficient user separation	3	[17], [18], [49]

	6. Maintainability Risks	#S	Sources
1	Incompatible with new technologies	17	[3], [4], [5], [9], [11], [14], [21], [22], [27], [28], [29], [34], [38], [41], [45], [56], [61]
2	Inflexibility regarding business change	14	[4], [5], [9], [14], [22], [27], [28], [29], [34], [38], [41], [45], [56], [61]
3	IT becomes undifferentiated commodity	8	[11], [14], [27], [28], [35], [43], [56], [64]
4	Incompatible business processes	6	[11], [16], [23], [35], [38], [59]
5	Proprietary technologies	6	[18], [20], [23], [27], [49], [52]
6	Costly modifications are necessary	4	[17], [38], [41], [52]
7	Insufficient maintenance	4	[8], [38], [41], [64]
8	Limited customization possibilities	3	[34], [36], [45]
9	Limited data import	3	[16], [18], [20]
10	Service does not perfectly fit	2	[34], [36]
11	Unfavorably timed updates	2	[41], [60]

A.3 Q-Sort Statistics

The following tables show detailled statistics of the Q-sort process carried out in section 3.2. While table A.3 shows the assignment of cards to the different dimensions, tables A.4 to A.7 contain the indiviual assignments for each of the three rounds, as well as for the final set of risk items. Table A.8 shows statistics for calculating the inter-rater reliabilities (Cohen's Kappa).

Table A.3 Q-Sort Class Hit Ratios

		Cards placed in Dimension							
	Target Dimension	Confidentiality	Integrity	Availability	Performance	Accountability	Maintainability	Unclear	Hit Rate
First Round	Confidentiality	29	0	0	0	0	0	1	96.7%
	Integrity	0	19	0	0	0	0	5	79.2%
	Availability	0	3	39	6	0	0	6	72.2%
	Performance	0	0	2	23	0	1	4	76.7%
	Accountability	7	3	0	0	17	0	3	56.7%
	Maintainability	0	0	0	3	0	41	22	62.1%
Second Round	Confidentiality	16	2	0	0	0	0	0	88.9%
	Integrity	0	24	0	0	0	0	0	100.0%
	Availability	0	1	33	2	0	0	0	91.7%
	Performance	0	0	0	21	0	3	0	87.5%
	Accountability	8	1	0	0	21	0	0	70.0%
	Maintainability	0	0	1	0	0	46	7	85.2%
Third Round	Confidentiality	16	2	0	0	0	0	0	88.9%
	Integrity	0	24	0	0	0	0	0	100.0%
	Availability	0	1	33	2	0	0	0	91.7%
	Performance	0	0	0	23	0	1	0	95.8%
	Accountability	1	2	0	0	27	0	0	90.0%
	Maintainability	0	0	1	0	0	46	7	85.2%
Final Risk Set	Confidentiality	16	2	0	0	0	0	0	88.9%
	Integrity	0	24	0	0	0	0	0	100.0%
	Availability	0	1	33	2	0	0	0	91.7%
	Performance	0	0	0	23	0	1	0	95.8%
	Accountability	1	2	0	0	27	0	0	90.0%
	Maintainability	0	0	1	0	0	41	0	97.6%

Table A.4 Q-Sort Assignments after First Round

Short Risk Item Description	Target	Judges						Placem. Ratio	Action
		1	2	3	4	5	6		
Supplier looking at sensitive data	1	1	1	1	1	1	1	100%	
Compromised data confidentially	1	?	1	1	1	1	1	83%	R
Disclosure of data by the provider	1	1	1	1	1	1	1	100%	
Insufficient protection against eavesdropping	1	1	1	1	1	1	1	100%	
Eavesdropping communications	1	1	1	1	1	1	1	100%	R
Data manipulation at provider side	2	2	2	2	?	2	2	83%	
Accidental modifications of transferred data	2	2	2	2	?	2	2	83%	
Manipulation of transferred data	2	2	2	2	2	2	2	100%	
Accidental data modifications at provider side	2	2	?	2	?	?	2	50%	P
Discontinuity of the service	3	3	3	3	3	3	?	83%	
Insufficient availability and low uptime	3	3	3	2	4	4	3	50%	M
Unintentional downtime	3	3	3	2	4	4	3	50%	M
Insufficient protection against downtime	3	3	3	3	3	3	3	100%	
Service delivery problems	3	3	?	?	4	3	?	33%	R
Loss of data access	3	3	3	3	3	3	?	83%	
Technical issues and system failures	3	3	3	3	4	3	3	83%	
Attacks against availability	3	3	3	3	3	3	3	100%	
Data loss at provider side	3	3	3	3	?	3	2	67%	P
Network performance problems	4	4	3	3	4	4	4	67%	P
Limited scalability	4	4	4	?	?	6	4	50%	P
Deliberate underperformance	4	4	?	4	4	4	?	67%	P
Insufficient service performance	4	4	4	4	4	4	4	100%	R
Insufficient protection against underperformance	4	4	4	4	4	4	4	100%	
Access without authorization	5	1	1	1	1	?	5	17%	P
Attackers generate costs	5	5	5	5	5	5	5	100%	
Identity theft	5	1	5	1	5	2	5	50%	P
Insufficient logging of actions	5	5	5	5	2	5	5	83%	
Insufficient user separation	5	?	?	5	2	1	5	33%	P
Incompatible with new technologies	6	6	6	6	6	6	6	100%	
Inflexibility regarding business change	6	6	6	6	6	6	6	100%	M
IT becomes undifferentiated commodity	6	4	?	?	?	?	?	0%	P
Incompatible business processes	6	6	6	4	?	?	?	33%	P
Proprietary technologies	6	6	6	6	6	6	?	83%	
Costly modifications are necessary	6	6	6	6	6	6	?	83%	R
Insufficient maintenance	6	6	?	?	6	6	6	67%	P
Limited customization possibilities	6	6	6	6	6	6	6	100%	
Limited data import	6	6	6	6	6	6	6	100%	
Service does not perfectly fit	6	?	?	4	?	?	?	0%	P
Unfavorably timed updates	6	6	?	?	?	?	?	17%	P

The actions were: R: remove item, M: merge item with another item, P: change phrasing of item.

Table A.5 Q-Sort Assignments after Second Round

Short Risk Item Description	Target	Judges						Placem. Ratio	Action
		1	2	3	4	5	6		
Supplier looking at sensitive data	1	1	1	1	1	1	1	100%	
Disclosure of data by the provider	1	1	1	1	1	2	1	83%	
Insufficient protection against eavesdropping	1	1	1	1	1	2	1	83%	
Data manipulation at provider side	2	2	2	2	2	2	2	100%	
Accidental modifications of transferred data	2	2	2	2	2	2	2	100%	
Manipulation of transferred data	2	2	2	2	2	2	2	100%	
Accidental data modifications at provider side	2	2	2	2	2	2	2	100%	
Discontinuity of the service	3	3	3	3	3	3	3	100%	
Insufficient protection against downtime	3	3	3	3	3	3	3	100%	
Loss of data access	3	3	3	3	3	3	3	100%	
Unintentional downtime	3	3	3	4	3	3	3	83%	
Attacks against availability	3	3	3	3	3	4	3	83%	
Data loss at provider side	3	3	3	3	3	3	2	83%	
Network performance problems	4	4	4	4	4	4	4	100%	
Limited scalability	4	4	4	4	6	6	6	50%	P
Deliberate underperformance	4	4	4	4	4	4	4	100%	
Insufficient protection against underperformance	4	4	4	4	4	4	4	100%	
Access without authorization	5	1	1	5	5	1	1	33%	P
Attackers generate costs	5	5	5	5	5	5	5	100%	
Identity theft	5	1	1	5	5	1	5	50%	P
Insufficient logging of actions	5	5	5	5	5	5	5	100%	
Insufficient user separation	5	1	5	5	5	2	5	67%	P
Incompatible with new technologies	6	6	6	6	6	6	6	100%	
IT becomes undifferentiated commodity	6	6	?	?	?	6	?	33%	P
Incompatible business processes	6	6	6	6	6	6	6	100%	
Proprietary technologies	6	6	3	6	6	6	6	83%	
Insufficient maintenance	6	6	6	6	6	6	6	100%	
Limited customization possibilities	6	6	6	6	6	6	6	100%	
Limited data import	6	6	6	6	6	6	6	100%	
Service does not perfectly fit	6	?	6	?	6	6	?	50%	P
Unfavorably timed updates	6	6	6	6	6	6	6	100%	

The action was: P: change phrasing of item.

Table A.6 Q-Sort Assignments after Third Round

Short Risk Item Description	Target	Judges						Placem. Ratio	Action
		1	2	3	4	5	6		
Supplier looking at sensitive data	1	1	1	1	1	1	1	100%	
Disclosure of data by the provider	1	1	1	1	1	2	1	83%	
Insufficient protection against eavesdropping	1	1	1	1	1	2	1	83%	
Data manipulation at provider side	2	2	2	2	2	2	2	100%	
Accidental modifications of transferred data	2	2	2	2	2	2	2	100%	
Manipulation of transferred data	2	2	2	2	2	2	2	100%	
Accidental data modifications at provider side	2	2	2	2	2	2	2	100%	
Discontinuity of the service	3	3	3	3	3	3	3	100%	
Insufficient protection against downtime	3	3	3	3	3	3	3	100%	
Loss of data access	3	3	3	3	3	3	3	100%	
Unintentional downtime	3	3	3	4	3	3	3	83%	
Attacks against availability	3	3	3	3	3	4	3	83%	
Data loss at provider side	3	3	3	3	3	3	2	83%	
Network performance problems	4	4	4	4	4	4	4	100%	
Limited scalability	4	4	4	4	4	6	4	83%	
Deliberate underperformance	4	4	4	4	4	4	4	100%	
Insufficient protection against underperformance	4	4	4	4	4	4	4	100%	
Access without authorization	5	5	5	2	5	5	5	83%	
Attackers generate costs	5	5	5	5	5	5	5	100%	
Identity theft	5	5	1	5	5	5	5	83%	
Insufficient logging of actions	5	5	5	5	5	5	5	100%	
Insufficient user separation	5	5	5	2	5	5	5	83%	
Incompatible with new technologies	6	6	6	6	6	6	6	100%	
IT becomes undifferentiated commodity	6	6	?	?	?	6	?	33%	R
Incompatible business processes	6	6	6	6	6	6	6	100%	
Proprietary technologies	6	6	3	6	6	6	6	83%	
Insufficient maintenance	6	6	6	6	6	6	6	100%	
Limited customization possibilities	6	6	6	6	6	6	6	100%	
Limited data import	6	6	6	6	6	6	6	100%	
Service does not perfectly fit	6	?	6	?	6	6	?	50%	R
Unfavorably timed updates	6	6	6	6	6	6	6	100%	

The action was: R: remove item.

Table A.7 Q-Sort Assignments with Final Risk Set

Short Risk Item Description	Target	Judges						Placem. Ratio
		1	2	3	4	5	6	
Supplier looking at sensitive data	1	1	1	1	1	1	1	100%
Disclosure of data by the provider	1	1	1	1	1	2	1	83%
Insufficient protection against eavesdropping	1	1	1	1	1	2	1	83%
Data manipulation at provider side	2	2	2	2	2	2	2	100%
Accidental modifications of transferred data	2	2	2	2	2	2	2	100%
Manipulation of transferred data	2	2	2	2	2	2	2	100%
Accidental data modifications at provider side	2	2	2	2	2	2	2	100%
Discontinuity of the service	3	3	3	3	3	3	3	100%
Insufficient protection against downtime	3	3	3	3	3	3	3	100%
Loss of data access	3	3	3	3	3	3	3	100%
Unintentional downtime	3	3	3	4	3	3	3	83%
Attacks against availability	3	3	3	3	3	4	3	83%
Data loss at provider side	3	3	3	3	3	3	2	83%
Network performance problems	4	4	4	4	4	4	4	100%
Limited scalability	4	4	4	4	4	6	4	83%
Deliberate underperformance	4	4	4	4	4	4	4	100%
Insufficient protection against underperformance	4	4	4	4	4	4	4	100%
Access without authorization	5	5	5	2	5	5	5	83%
Attackers generate costs	5	5	5	5	5	5	5	100%
Identity theft	5	5	1	5	5	5	5	83%
Insufficient logging of actions	5	5	5	5	5	5	5	100%
Insufficient user separation	5	5	5	2	5	5	5	83%
Incompatible with new technologies	6	6	6	6	6	6	6	100%
Incompatible business processes	6	6	6	6	6	6	6	100%
Proprietary technologies	6	6	3	6	6	6	6	83%
Insufficient maintenance	6	6	6	6	6	6	6	100%
Limited customization possibilities	6	6	6	6	6	6	6	100%
Limited data import	6	6	6	6	6	6	6	100%
Unfavorably timed updates	6	6	6	6	6	6	6	100%

Table A.8 Q-Sort Cohen's Kappas

Judges		Round 1 Agreements (out of 39)	Round 1 Kappa	Round 2 Agreements (out of 31)	Round 2 Kappa	Round 3 Agreements (out of 31)	Round 3 Kappa	Final Risk Set Agreements (out of 29)	Final Risk Set Kappa
1	2	30	76.9%	27	87.1%	27	87.1%	27	93.1%
1	3	27	69.2%	26	83.9%	27	87.1%	26	89.7%
1	4	23	59.0%	25	80.6%	29	93.5%	29	100.0%
1	5	28	71.8%	25	80.6%	26	83.9%	25	86.2%
1	6	25	64.1%	26	83.9%	29	93.5%	28	96.6%
2	3	30	76.9%	26	83.9%	25	80.6%	24	82.8%
2	4	25	64.1%	27	87.1%	29	93.5%	27	93.1%
2	5	28	71.8%	24	77.4%	24	77.4%	23	79.3%
2	6	28	71.8%	26	83.9%	27	87.1%	26	89.7%
3	4	24	61.5%	28	90.3%	27	87.1%	26	89.7%
3	5	27	69.2%	21	67.7%	22	71.0%	22	75.9%
3	6	24	61.5%	27	87.1%	27	87.1%	25	86.2%
4	5	29	74.4%	24	77.4%	26	83.9%	25	86.2%
4	6	22	56.4%	28	90.3%	29	93.5%	28	96.6%
5	6	25	64.1%	23	74.2%	24	77.4%	24	82.8%
Avg.		26.3	67.5%	25.5	82.4%	26.5	85.6%	25.7	88.5%

A.4 Expert Interview Statistics

Table A.9 Expert Interview Details per Risk Item

Short Risk Item Description	"obviously part of"	"possibly part of"	"not part of"
Supplier looking at sensitive data	24 (100%)	0 (0%)	0 (0%)
Disclosure of data by the provider	20 (83%)	3 (13%)	1 (4%)
Eavesdropping communications	22 (92%)	2 (8%)	0 (0%)
Data manipulation at provider side	22 (92%)	2 (8%)	0 (0%)
Accidental modification of transferred data	18 (75%)	5 (21%)	1 (4%)
Manipulation of transferred data	22 (92%)	2 (8%)	0 (0%)
Accidental data modification at provider side	17 (71%)	6 (25%)	1 (4%)
Discontinuity of the service	20 (83%)	4 (17%)	0 (0%)
Insufficient protection against downtime	24 (100%)	0 (0%)	0 (0%)
Loss of data access	20 (83%)	3 (13%)	1 (4%)
Unintentional downtime	23 (96%)	1 (4%)	0 (0%)
Attacks against availability	21 (88%)	3 (13%)	0 (0%)
Data loss at provider side	20 (83%)	3 (13%)	1 (4%)
Network performance problems	21 (88%)	2 (8%)	1 (4%)
Limited scalability	22 (92%)	1 (4%)	1 (4%)
Deliberate underperformance	20 (83%)	4 (17%)	0 (0%)
Insufficient protection against underperformance	21 (88%)	3 (13%)	0 (0%)
Access without authorization	21 (88%)	3 (13%)	0 (0%)
Attackers generate costs	21 (88%)	3 (13%)	0 (0%)
Identity theft	21 (88%)	2 (8%)	1 (4%)
Insufficient logging of actions	21 (88%)	3 (13%)	0 (0%)
Insufficient user separation	22 (92%)	2 (8%)	0 (0%)
Incompatible with new technologies	19 (79%)	5 (21%)	0 (0%)
Incompatible business processes	21 (88%)	3 (13%)	0 (0%)
Proprietary technologies	20 (83%)	3 (13%)	1 (4%)
Insufficient maintenance	22 (92%)	2 (8%)	0 (0%)
Limited customization possibilities	21 (88%)	3 (13%)	0 (0%)
Limited data import	21 (88%)	3 (13%)	0 (0%)
Unfavorably timed updates	20 (83%)	4 (17%)	0 (0%)

A.5 Questionnaire Items

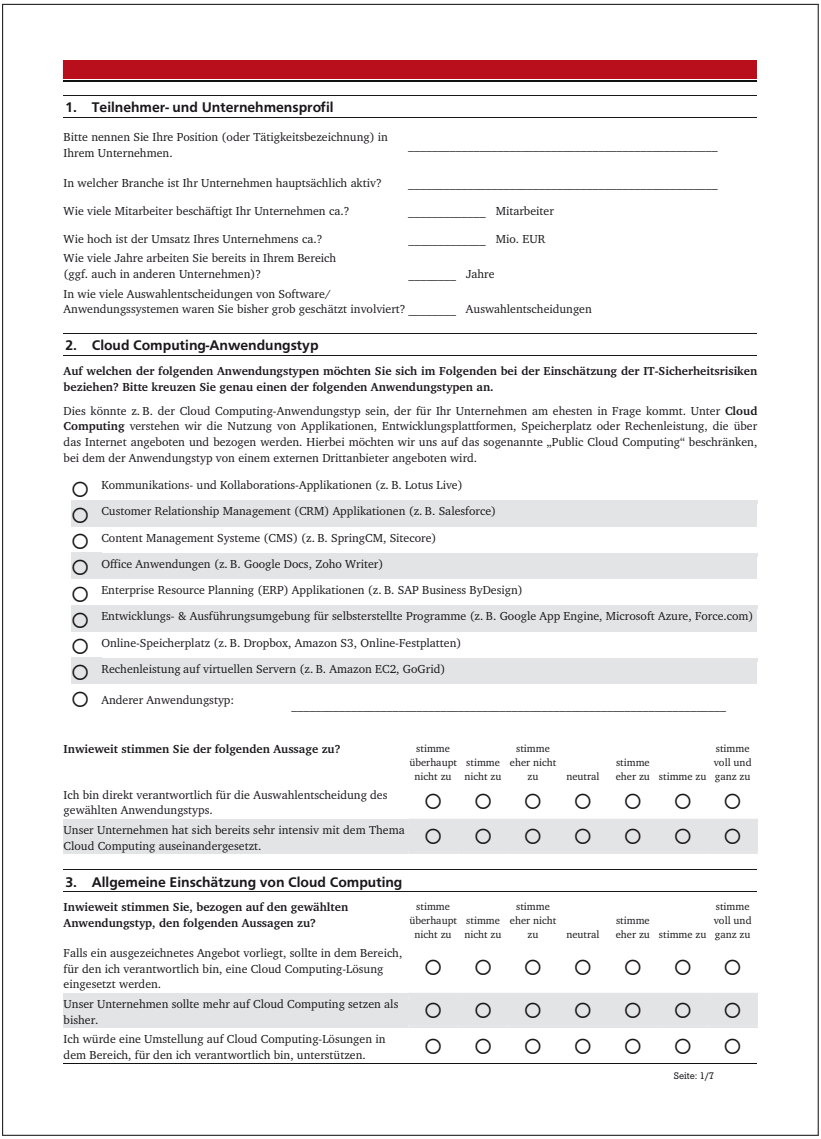
Table A.10 Questionnaire Items (1/2)

Constructs	Indicators
	In the course of using Cloud Computing, how does your company perceive the risk that ...
Perceived Confidentiality Risk	1: ... your transferred data are eavesdropped by unauthorized persons?
	2: ... your data are looked at by unauthorized persons on the supplier side?
	3: ... your data fall into the wrong hands because of disclosure by the provider?
	4: ... unauthorized persons can look at data on your internal systems (e. g., due to vulnerabilities of the browser or the used protocols)?
Perceived Integrity Risk	5: ... your data are manipulated during transmission?
	6: ... your data are manipulated at the provider side?
	7: ... your data are accidentally modified during the transfer, e. g., due to a network error?
	8: ... your data are accidentally modified at the provider side, e. g., due to a technical error?
	9: ... unauthorized persons modify data on your internal systems (e. g., through the interface to the provider)?
Perceived Availability Risk	10: ... the provisioning of the service is discontinued, e. g., due to insolvency of the provider?
	11: ... it comes to unintentional downtime, e. g., because of technical errors and system crashes?
	12: ... attacks are carried out which make the service unusable (so-called denial-of-service attacks)?
	13: ... you can no longer log on to the service and therefore lose access to your data?
	14: ... the provider experiences data loss and the data may not be recoverable?
	15: ... the availability of your internal systems is limited, e. g., during the data transfer to the provider?

Table A.11 Questionnaire Items (2/2)

Constructs	Indicators
	In the course of using Cloud Computing, how does your company perceive the risk that …
Perceived Performance Risk	16: … you experience performance problems with the network or the Internet, e. g., high response times or low data throughput?
	17: … the performance of the service is not adequate, as soon as your own or the whole intensity of use changes (especially increases)?
	18: … the provider shows deliberate underperformance below the levels stated before conclusion of the contract and therefore, e. g., speed or throughput decline?
	19: … you experience performance issues of your internal systems (e. g., during the data transfer to the provider)?
Perceived Accountability Risk	20: … after the theft of your login data, attackers perform actions in the system on your behalf?
	21: … the separation of users sharing the system is insufficient, so they can perform actions on behalf of other users?
	22: … the logging of performed actions (as part of your use, but also by an attacker) is insufficient, so that they cannot be accounted to the initiator afterwards?
	23: … it is possible to access the system without authorization (e. g., by individual usernames and passwords), so that performed actions cannot be accounted to the initiator afterwards?
	24: … actions can be performed on your internal systems (e. g., through the interface to the provider) which cannot be accounted to the initiator?
Perceived Maintainability Risk	25: … the service cannot be flexibly adapted to changes in business processes or the internally used software?
	26: … the business processes or the software on your side and the provider side are incompatible?
	27: … the offered service cannot be flexibly adapted to new technologies?
	28: … it is difficult to import existing data into the provisioned application type?
	29: … the provider uses proprietary technologies or does not offer possibilities to export data and thereby hampers the switch to another provider?
	30: … the provider insufficiently maintains the service and possibly realizes few improvements or does not further develop the software?
	31: … the provider rolls out unfavorably timed updates and therefore, e. g., used functionalities are dropped?

A.6 Survey Questionnaire



1. Teilnehmer- und Unternehmensprofil

Bitte nennen Sie Ihre Position (oder Tätigkeitsbezeichnung) in Ihrem Unternehmen. _____

In welcher Branche ist Ihr Unternehmen hauptsächlich aktiv? _____

Wie viele Mitarbeiter beschäftigt Ihr Unternehmen ca.? _____ Mitarbeiter

Wie hoch ist der Umsatz Ihres Unternehmens ca.? _____ Mio. EUR

Wie viele Jahre arbeiten Sie bereits in Ihrem Bereich (ggf. auch in anderen Unternehmen)? _____ Jahre

In wie viele Auswahlentscheidungen von Software/ Anwendungssystemen waren Sie bisher grob geschätzt involviert? _____ Auswahlentscheidungen

2. Cloud Computing-Anwendungstyp

Auf welchen der folgenden Anwendungstypen möchten Sie sich im Folgenden bei der Einschätzung der IT-Sicherheitsrisiken beziehen? Bitte kreuzen Sie genau einen der folgenden Anwendungstypen an.

Dies könnte z. B. der Cloud Computing-Anwendungstyp sein, der für Ihr Unternehmen am ehesten in Frage kommt. Unter **Cloud Computing** verstehen wir die Nutzung von Applikationen, Entwicklungsplattformen, Speicherplatz oder Rechenleistung, die über das Internet angeboten und bezogen werden. Hierbei möchten wir uns auf das sogenannte „Public Cloud Computing" beschränken, bei dem der Anwendungstyp von einem externen Drittanbieter angeboten wird.

- ○ Kommunikations- und Kollaborations-Applikationen (z. B. Lotus Live)
- ○ Customer Relationship Management (CRM) Applikationen (z. B. Salesforce)
- ○ Content Management Systeme (CMS) (z. B. SpringCM, Sitecore)
- ○ Office Anwendungen (z. B. Google Docs, Zoho Writer)
- ○ Enterprise Resource Planning (ERP) Applikationen (z. B. SAP Business ByDesign)
- ○ Entwicklungs- & Ausführungsumgebung für selbsterstellte Programme (z. B. Google App Engine, Microsoft Azure, Force.com)
- ○ Online-Speicherplatz (z. B. Dropbox, Amazon S3, Online-Festplatten)
- ○ Rechenleistung auf virtuellen Servern (z. B. Amazon EC2, GoGrid)
- ○ Anderer Anwendungstyp: _____

Inwieweit stimmen Sie der folgenden Aussage zu?	stimme überhaupt nicht zu	stimme nicht zu	stimme eher nicht zu	neutral	stimme eher zu	stimme zu	stimme voll und ganz zu
Ich bin direkt verantwortlich für die Auswahlentscheidung des gewählten Anwendungstyps.	○	○	○	○	○	○	○
Unser Unternehmen hat sich bereits sehr intensiv mit dem Thema Cloud Computing auseinandergesetzt.	○	○	○	○	○	○	○

3. Allgemeine Einschätzung von Cloud Computing

Inwieweit stimmen Sie, bezogen auf den gewählten Anwendungstyp, den folgenden Aussagen zu?	stimme überhaupt nicht zu	stimme nicht zu	stimme eher nicht zu	neutral	stimme eher zu	stimme zu	stimme voll und ganz zu
Falls ein ausgezeichnetes Angebot vorliegt, sollte in dem Bereich, für den ich verantwortlich bin, eine Cloud Computing-Lösung eingesetzt werden.	○	○	○	○	○	○	○
Unser Unternehmen sollte mehr auf Cloud Computing setzen als bisher.	○	○	○	○	○	○	○
Ich würde eine Umstellung auf Cloud Computing-Lösungen in dem Bereich, für den ich verantwortlich bin, unterstützen.	○	○	○	○	○	○	○

Seite: 1/7

Figure A.1 Survey Questionnaire - Page 1 of 7

Inwieweit stimmen Sie, bezogen auf den gewählten Anwendungstyp, den folgenden Aussagen zu?	stimme überhaupt nicht zu	stimme nicht zu	stimme eher nicht zu	neutral	stimme eher zu	stimme zu	stimme voll und ganz zu
Der Bezug von Cloud Computing-Lösungen ist mit hohen Risiken verbunden.	○	○	○	○	○	○	○
Das Risiko ist hoch, dass erhoffte Einsparungen (erzielt durch die Umstellung auf Cloud Computing) ausbleiben.	○	○	○	○	○	○	○
Insgesamt sehe ich den Bezug von Cloud Computing-Lösungen als gefährlich an.	○	○	○	○	○	○	○
Der Bezug von Cloud Computing-Lösungen hat viele Vorteile.	○	○	○	○	○	○	○
Der Bezug von Cloud Computing-Lösungen ist ein nützliches Instrument zur Senkung der operativen Kosten in unserem Unternehmen.	○	○	○	○	○	○	○
Insgesamt sehe ich den Einsatz von Cloud Computing als eine zweckdienliche strategische Option an.	○	○	○	○	○	○	○

4. Intensität heutiger und zukünftiger Nutzung

Welchen Anteil des IT-Budgets für den gewählten Anwendungstyp investieren Sie in Cloud Computing?

Jahr **2011** (geschätzt in %): _____ %

Jahr **2014** (geschätzt in %): _____ %

Inwieweit nutzen Sie Cloud Computing für den Bezug des gewählten Anwendungstyps?	überhaupt nicht	fast nicht	eher nicht	neutral	eher schon	viel	voll und ganz
Jahr 2011	○	○	○	○	○	○	○
Jahr 2014	○	○	○	○	○	○	○

Alles in allem bewertet unser Unternehmen den Bezug des gewählten Anwendungstyps über ein Cloud Computing-Modell als:

negativ	○	○	○	○	○	○	○	positiv
schädlich	○	○	○	○	○	○	○	nutzenstiftend
unwichtig	○	○	○	○	○	○	○	wichtig

Personen (z. B. Experten) oder Gruppen (z. B. Branchenverbände), deren Meinung uns wichtig ist, bewerten den Bezug des gewählten Anwendungstyps über ein Cloud Computing-Modell als:

negativ	○	○	○	○	○	○	○	positiv
schädlich	○	○	○	○	○	○	○	nutzenstiftend
unwichtig	○	○	○	○	○	○	○	wichtig

Figure A.2 Survey Questionnaire - Page 2 of 7

5. Verfügbarkeits-Risiken

Bitte bewerten Sie, bezogen auf den gewählten Anwendungstyp, folgende Risiken aus dem Bereich **Verfügbarkeit**. Hierunter verstehen wir, dass der Zugriff auf das Angebot und die Daten zu jedem (vom Kunden gewünschten) Zeitpunkt möglich ist. In die Bewertung eines Risikos sollten sowohl Eintrittswahrscheinlichkeit des Ereignisses als auch dessen negativen Auswirkungen, wie etwa die potentiellen Schäden, einfließen.

Wie bewertet Ihr Unternehmen im Zuge der Nutzung von Cloud Computing das Risiko, dass …	überhaupt nicht riskant	nicht riskant	eher nicht riskant	indifferent	eher riskant	riskant	überaus riskant
… die Bereitstellung des Angebots eingestellt wird, z. B. aufgrund einer Insolvenz des Anbieters?	○	○	○	○	○	○	○
… es zu ungewollten Ausfällen und damit verbundener Downtime kommt, z. B. aufgrund von technischen Fehlern und Systemabstürzen?	○	○	○	○	○	○	○
… bewusste Angriffe durchführt werden, die das Angebot arbeitsunfähig machen (sogenannte Denial-of-Service-Angriffe)?	○	○	○	○	○	○	○
… Sie sich nicht mehr bei dem Angebot anmelden können und deswegen den Zugriff auf Ihre Daten verlieren?	○	○	○	○	○	○	○
… es auf Anbieterseite zu Datenverlusten kommt und sich die Daten evtl. nicht wiederherstellen lassen?	○	○	○	○	○	○	○
… (z. B. während des Datentransfers zum Anbieter) die Verfügbarkeit Ihrer internen Systeme beeinträchtigt wird?	○	○	○	○	○	○	○

Bitte vervollständigen Sie die folgende Aussage: In Bezug auf die Verfügbarkeit Ihrer Systeme und Daten wäre es für Ihr Unternehmen …, Cloud Computing zu nutzen.

überhaupt nicht riskant	○	○	○	○	○	○	○	überaus riskant
überhaupt nicht gefährlich	○	○	○	○	○	○	○	überaus gefährlich
mit sehr geringen Unsicherheiten verbunden	○	○	○	○	○	○	○	mit sehr großen Unsicherheiten verbunden

6. Vertraulichkeits-Risiken

Bitte bewerten Sie, bezogen auf den gewählten Anwendungstyp, folgende Risiken aus dem Bereich **Vertraulichkeit**. Hierunter verstehen wir, dass Daten ausschließlich von autorisierten Benutzern gelesen werden.

Wie bewertet Ihr Unternehmen im Zuge der Nutzung von Cloud Computing das Risiko, dass …	überhaupt nicht riskant	nicht riskant	eher nicht riskant	indifferent	eher riskant	riskant	überaus riskant
… Ihre Daten während der Übertragung von Unbefugten abgehört werden?	○	○	○	○	○	○	○
… Ihre Daten auf Anbieterseite von Unbefugten eingesehen werden?	○	○	○	○	○	○	○
… Ihre Daten, aufgrund der Weitergabe durch den Anbieter, in die Hände von unbefugten Dritten gelangen?	○	○	○	○	○	○	○
… Unbefugte (z. B. durch Schwachstellen im Browser oder den Protokollen) Daten auf Ihren internen Systemen einsehen?	○	○	○	○	○	○	○

Bitte vervollständigen Sie die folgende Aussage: In Bezug auf die Vertraulichkeit Ihrer Systeme und Daten wäre es für Ihr Unternehmen …, Cloud Computing zu nutzen.

überhaupt nicht riskant	○	○	○	○	○	○	○	überaus riskant
überhaupt nicht gefährlich	○	○	○	○	○	○	○	überaus gefährlich
mit sehr geringen Unsicherheiten verbunden	○	○	○	○	○	○	○	mit sehr großen Unsicherheiten verbunden

Seite: 3/7

Figure A.3 Survey Questionnaire - Page 3 of 7

7. Integritäts-Risiken

Bitte bewerten Sie, bezogen auf den gewählten Anwendungstyp, folgende Risiken aus dem Bereich **Integrität**. Hierunter verstehen wir, dass Daten nicht von Unbefugten verändert, z. B. manipuliert, werden.

Wie bewertet Ihr Unternehmen im Zuge der Nutzung von Cloud Computing das Risiko, dass …	überhaupt nicht riskant	nicht riskant	eher nicht riskant	indifferent	eher riskant	riskant	überaus riskant
… Ihre Daten während der Übertragung manipuliert werden?	○	○	○	○	○	○	○
… Ihre Daten beim Anbieter manipuliert werden?	○	○	○	○	○	○	○
… Ihre Daten während der Übertragung unbeabsichtigt verändert werden, z. B. durch einen Netzwerkfehler?	○	○	○	○	○	○	○
… Ihre Daten beim Anbieter unbeabsichtigt verändert werden, z. B. durch einen technischen Fehler?	○	○	○	○	○	○	○
… Unbefugte (z. B. über die Schnittstelle zum Anbieter) Daten auf Ihren internen Systemen verändern?	○	○	○	○	○	○	○

Bitte vervollständigen Sie die folgende Aussage: In Bezug auf die Integrität Ihrer Systeme und Daten wäre es für Ihr Unternehmen …, Cloud Computing zu nutzen.

überhaupt nicht riskant	○	○	○	○	○	○	○	überaus riskant
überhaupt nicht gefährlich	○	○	○	○	○	○	○	überaus gefährlich
mit sehr geringen Unsicherheiten verbunden	○	○	○	○	○	○	○	mit sehr großen Unsicherheiten verbunden

8. Leistungs-Risiken

Bitte bewerten Sie, bezogen auf den gewählten Anwendungstyp, folgende Risiken aus dem Bereich **Leistung**. Hierunter verstehen wir, dass die Nutzung des Angebots und der Daten in der Geschwindigkeit erfolgen kann, die den Leistungsanforderungen der Kunden entspricht.

Wie bewertet Ihr Unternehmen im Zuge der Nutzung von Cloud Computing das Risiko, dass …	überhaupt nicht riskant	nicht riskant	eher nicht riskant	indifferent	eher riskant	riskant	überaus riskant
… Geschwindigkeitsprobleme mit dem Netzwerk oder Internet auftreten, z. B. hohe Antwortzeiten oder geringer Datendurchsatz?	○	○	○	○	○	○	○
… die Leistung des Angebots nicht adäquat ist sobald sich die eigene oder auch die gesamte Nutzungsintensität des Angebots verändert (insbesondere ansteigt)?	○	○	○	○	○	○	○
… der Anbieter nach Vertragsabschluss bewusst geringere Leistungen anbietet als vor Vertragsabschluss dargestellt oder versprochen, und daher z. B. die Geschwindigkeit oder der Durchsatz abnehmen?	○	○	○	○	○	○	○
… (z. B. während des Datentransfers zum Anbieter) die Geschwindigkeit Ihrer internen Systeme beeinträchtigt wird?	○	○	○	○	○	○	○

Bitte vervollständigen Sie die folgende Aussage: In Bezug auf die Leistung Ihrer Systeme und Daten wäre es für Ihr Unternehmen …, Cloud Computing zu nutzen.

überhaupt nicht riskant	○	○	○	○	○	○	○	überaus riskant
überhaupt nicht gefährlich	○	○	○	○	○	○	○	überaus gefährlich
mit sehr geringen Unsicherheiten verbunden	○	○	○	○	○	○	○	mit sehr großen Unsicherheiten verbunden

Figure A.4 Survey Questionnaire - Page 4 of 7

9. Anpassbarkeits- und Wartungs-Risiken

Bitte bewerten Sie, bezogen auf den gewählten Anwendungstyp, folgende Risiken aus dem Bereich **Anpassbarkeit und Wartung**. Hierunter verstehen wir, dass Anpassungen des Angebots an eigene bzw. geänderte Anforderungen möglich und Wartung sowie Support gewährleistet sind.

Wie bewertet Ihr Unternehmen im Zuge der Nutzung von Cloud Computing das Risiko, dass …	überhaupt nicht riskant	nicht riskant	eher nicht riskant	indiff-erent	eher riskant	riskant	überaus riskant
… das Angebot nicht flexibel an Änderungen der Geschäftsprozesse oder der intern genutzten Software angepasst werden kann?	○	○	○	○	○	○	○
… die Geschäftsprozesse oder Software auf Ihrer und Anbieterseite inkompatibel sind?	○	○	○	○	○	○	○
… das Angebot nicht flexibel an neue Technologien angepasst werden kann?	○	○	○	○	○	○	○
… es schwer ist, bestehende Daten in das Angebot zu importieren?	○	○	○	○	○	○	○
… der Anbieter proprietäre Technologien einsetzt und dadurch einen Anbieterwechsel behindert, bzw. keine Möglichkeit vorsieht, um Daten zu exportieren?	○	○	○	○	○	○	○
… der Anbieter nicht ausreichend Wartung leistet und evtl. wenige Verbesserungen umsetzt bzw. die Software nicht weiterentwickelt?	○	○	○	○	○	○	○
… der Anbieter Updates zu einem ungünstigen Zeitpunkt einspielt und beispielsweise deswegen genutzte Funktionen entfallen?	○	○	○	○	○	○	○

Bitte vervollständigen Sie die folgende Aussage: In Bezug auf die Anpassbarkeit und Wartung Ihrer Systeme und Daten wäre es für Ihr Unternehmen …, Cloud Computing zu nutzen.

überhaupt nicht riskant	○	○	○	○	○	○	○	überaus riskant
überhaupt nicht gefährlich	○	○	○	○	○	○	○	überaus gefährlich
mit sehr geringen Unsicherheiten verbunden	○	○	○	○	○	○	○	mit sehr großen Unsicherheiten verbunden

10. Zurechenbarkeits-Risiken

Bitte bewerten Sie, bezogen auf den gewählten Anwendungstyp, folgende Risiken aus dem Bereich **Zurechenbarkeit**. Hierunter verstehen wir, dass Authentifizierungsmechanismen nicht umgangen werden können und Aktionen im Rahmen der Nutzung des Angebots und der Daten identifizierbaren Benutzern eindeutig zugeordnet werden können.

Wie bewertet Ihr Unternehmen im Zuge der Nutzung von Cloud Computing das Risiko, dass …	überhaupt nicht riskant	nicht riskant	eher nicht riskant	indiff-erent	eher riskant	riskant	überaus riskant
… nach dem Diebstahl Ihrer Anmeldedaten, Angreifer unter Ihrem Namen Aktionen im System durchführen?	○	○	○	○	○	○	○
… die Benutzer, die sich ein System teilen, nicht ausreichend voneinander getrennt sind und so im Namen eines anderen Kunden Aktionen durchführen können?	○	○	○	○	○	○	○
… durchgeführte Aktionen (im Rahmen Ihrer Nutzung, aber auch durch Angreifer) nur unzureichend protokolliert werden, so dass sie im Nachhinein nicht mehr den Verursachern zurechenbar sind?	○	○	○	○	○	○	○
… ohne individuelle Autorisation (z. B. durch persönlichen Benutzernamen und Passwort) auf das System zugegriffen wird und so Aktionen den Verursachern nicht zugeordnet werden können?	○	○	○	○	○	○	○
… (z. B. über die Schnittstelle zum Anbieter) Aktionen an Ihren internen Systemen durchgeführt werden, die keinem Verursacher zurechenbar sind?	○	○	○	○	○	○	○

Figure A.5 Survey Questionnaire - Page 5 of 7

Bitte vervollständigen Sie die folgenden Aussage: In Bezug auf die Zurechenbarkeit der Nutzung Ihrer Systeme und Daten wäre es für Ihr Unternehmen …, Cloud Computing zu nutzen.

überhaupt nicht riskant	○	○	○	○	○	○	○	überaus riskant
überhaupt nicht gefährlich	○	○	○	○	○	○	○	überaus gefährlich
mit sehr geringen Unsicherheiten verbunden	○	○	○	○	○	○	○	mit sehr großen Unsicherheiten verbunden

11. IT-Sicherheitsrisiken von Cloud Computing im Allgemeinen

Bitte vervollständigen Sie die folgenden Aussagen zu **IT-Sicherheitsrisiken im Allgemeinen** beim Bezug des gewählten Anwendungstyps im Rahmen von Cloud Computing, **zusammenfassend unter Berücksichtigung aller Faktoren, die die Sicherheit Ihrer IT betreffen**.

Für unsere allgemeine IT-Sicherheit wäre es …, Cloud Computing zu nutzen.

überhaupt nicht riskant	○	○	○	○	○	○	○	überaus riskant
überhaupt nicht gefährlich	○	○	○	○	○	○	○	überaus gefährlich
mit sehr geringen Unsicherheiten verbunden	○	○	○	○	○	○	○	mit sehr großen Unsicherheiten verbunden
mit überaus geringen Bedrohungen verbunden	○	○	○	○	○	○	○	mit überaus großen Bedrohungen verbunden

Inwieweit stimmen Sie, bezogen auf den gewählten Anwendungstyp, den folgenden Aussagen zu?	stimme überhaupt nicht zu	stimme nicht zu	stimme eher nicht zu	neutral	stimme eher zu	stimme zu	stimme voll und ganz zu
Die Schnittstelle zum Cloud Computing-Anbieter ist ein großes IT-Sicherheitsrisiko für unsere internen Systeme.	○	○	○	○	○	○	○
Der gewählte Anwendungstyp ist für unser Unternehmen geschäftskritisch.	○	○	○	○	○	○	○
Die Nutzung von Cloud Computing für den Bezug des gewählten Anwendungstyps setzt unser Unternehmen **keinen** IT-Sicherheitsrisiken aus.	○	○	○	○	○	○	○
Die von unserem Unternehmen genutzte Anwendung des gewählten Typs ist groß und komplex.	○	○	○	○	○	○	○

12. Selbsteinstufungen des Unternehmens

Beantworten Sie die folgenden Fragen bitte so, dass Sie die Perspektive Ihres Unternehmens möglichst gut wiedergeben.

Inwieweit stimmen Sie den folgenden Aussagen zu?	stimme überhaupt nicht zu	stimme nicht zu	stimme eher nicht zu	neutral	stimme eher zu	stimme zu	stimme voll und ganz zu
Wenn unser Unternehmen von einer neuen Technologie erfährt, suchen wir nach Möglichkeiten, mit ihr zu experimentieren.	○	○	○	○	○	○	○
Verglichen mit anderen Unternehmen aus unserer Branche ist unser Unternehmen meistens das Erste, welches neue Technologien ausprobiert.	○	○	○	○	○	○	○
Unser Unternehmen testet regelmäßig neue Technologien.	○	○	○	○	○	○	○

Inwieweit stimmen Sie den folgenden Aussagen zu?	stimme überhaupt nicht zu	stimme nicht zu	stimme eher nicht zu	neutral	stimme eher zu	stimme zu	stimme voll und ganz zu
Das wesentliche Ziel unserer Unternehmensstrategie ist die Erhöhung der Qualität unseres Kundenservices.	○	○	○	○	○	○	○

Seite: 6/7

Figure A.6 Survey Questionnaire - Page 6 of 7

Inwieweit stimmen Sie den folgenden Aussagen zu?	stimme überhaupt nicht zu	stimme nicht zu	stimme eher nicht zu	neutral	stimme eher zu	stimme zu	stimme voll und ganz zu
Meine Ansprüche und Wünsche werden bei der Planung des Mitarbeiter-Bonus-Programms miteinbezogen.	○	○	○	○	○	○	○
Ein spezialisierter Anbieter für den gewählten Anwendungstyp kann die Gesamtheit der Risiken besser kontrollieren als unser Unternehmen es bei einem internen Betrieb der Anwendung könnte.	○	○	○	○	○	○	○

Inwieweit stimmen Sie den folgenden Aussagen zu?	stimme überhaupt nicht zu	stimme nicht zu	stimme eher nicht zu	neutral	stimme eher zu	stimme zu	stimme voll und ganz zu
Unser Unternehmen ist bereit, für eine größere Belohnung auch größere Risiken in Kauf zu nehmen.	○	○	○	○	○	○	○
Unser Unternehmen mag es, Risiken einzugehen, obwohl es dabei scheitern könnte.	○	○	○	○	○	○	○
Unser Unternehmen setzt ein Vorhaben am liebsten dann um, wenn ganz sicher ist, dass es erfolgreich sein wird.	○	○	○	○	○	○	○
Unser Unternehmen bevorzugt einen getesteten und bewährten Ansatz gegenüber einem neuen Konzept, obwohl das neue Konzept unter Umständen zu einem besseren Ergebnis führen könnte.	○	○	○	○	○	○	○

13. (Optional) Individueller Ergebnisbericht und Gewinnspiel

Als Dankeschön verlosen wir unter allen Teilnehmern ein Apple iPad 2. Zudem stellen wir Ihnen gerne einen individuellen Ergebnisbericht zur Verfügung. Die folgenden Fragen sind optional und Ihre Antworten werden **nicht** mit den vorherigen Antworten in Verbindung gebracht. Unsere klaren Datenschutzbestimmungen finden Sie unter http://www.is.tu-darmstadt.de/cloudrisiken/.

Wenn Sie an der Verlosung eines Apple iPad 2 teilnehmen möchten, geben Sie bitte Ihre E-Mail-Adresse an: _____

Wenn Sie einen Ergebnisbericht dieser Studie erhalten möchten, geben Sie bitte Ihre E-Mail-Adresse an: _____

Falls Sie Fragen oder Anregungen bezüglich der Umfrage haben, können Sie uns diese gerne hier mitteilen:

Herzlichen Dank für Ihre Teilnahme

Den ausgefüllten Fragebogen können Sie entweder per Post im beigefügten Rückumschlag, per Fax oder per E-Mail an uns zurücksenden:

Post: TU Darmstadt – CASED
Prof. Dr. Peter Buxmann
Mornewegstr. 32
64293 Darmstadt

Fax: 06151 16 4825

E-Mail: peter.buxmann@is.tu-darmstadt.de

Onlineumfrage: http://www.is.tu-darmstadt.de/cloudrisiken/

Figure A.7 Survey Questionnaire - Page 7 of 7

A.7 Descriptive Sample Characteristics

Table A.12 Descriptive Sample Characteristics – Formative Indicators

Indicator	N	Mean	Median	St. Dev.	Var.	Min.	Max.
1	368	4.707	5	1.447	2.093	1	7
2	368	5.231	6	1.446	2.091	2	7
3	368	5.063	5	1.496	2.239	1	7
4	368	5.046	5	1.422	2.022	1	7
5	362	3.818	4	1.374	1.889	1	7
6	362	3.845	4	1.467	2.153	1	7
7	362	3.776	4	1.473	2.169	1	7
8	362	4.083	4	1.452	2.109	1	7
9	362	4.177	4	1.463	2.140	1	7
10	373	4.622	5	1.470	2.160	1	7
11	373	4.796	5	1.450	2.104	2	7
12	373	5.252	5	1.344	1.807	1	7
13	373	4.590	5	1.505	2.264	1	7
14	373	4.365	5	1.633	2.668	1	7
15	373	4.080	4	1.534	2.354	1	7
16	361	4.889	5	1.388	1.927	1	7
17	361	4.294	4	1.347	1.814	1	7
18	361	3.981	4	1.425	2.030	1	7
19	361	3.845	4	1.462	2.137	1	7
20	356	5.289	5	1.325	1.755	1	7
21	356	4.011	4	1.535	2.355	1	7
22	356	4.669	5	1.431	2.048	1	7
23	356	4.272	5	1.469	2.159	1	7
24	356	4.430	5	1.512	2.285	1	7
25	357	4.459	5	1.446	2.092	1	7
26	357	4.162	4	1.505	2.266	1	7
27	357	3.944	4	1.413	1.997	1	7
28	357	3.894	4	1.428	2.039	1	7
29	357	4.630	5	1.589	2.526	1	7
30	357	4.028	4	1.361	1.853	1	7
31	357	4.140	4	1.498	2.244	1	7

Table A.13 Descriptive Sample Characteristics – Reflective Indicators

Indicator	N	Mean	Median	St. Dev.	Var.	Min.	Max.
Conf1	368	5.405	6	1.262	1.593	2	7
Conf2	368	5.272	5	1.282	1.643	2	7
Inte1	362	4.646	5	1.387	1.924	1	7
Inte2	362	4.608	5	1.405	1.973	1	7
Avai1	373	4.928	5	1.409	1.987	1	7
Avai2	373	4.802	5	1.414	1.998	1	7
Perf1	361	4.548	5	1.376	1.893	1	7
Perf2	361	4.548	5	1.420	2.015	1	7
Acco1	356	4.795	5	1.249	1.561	1	7
Acco2	356	4.798	5	1.258	1.582	1	7
Main1	357	4.485	5	1.379	1.902	1	7
Main2	357	4.473	5	1.409	1.986	1	7
PITSR1	356	5.006	5	1.254	1.572	1	7
PITSR2	356	5.048	5	1.240	1.539	1	7
PITSR3	356	4.823	5	1.217	1.481	1	7
PNU1	354	5.291	5	1.236	1.527	1	7
PNU2	354	4.619	5	1.325	1.755	1	7
PNU3	354	4.763	5	1.477	2.181	1	7
PPU1	354	4.370	4	1.265	1.599	1	7
PPU2	354	4.110	4	1.322	1.747	1	7
PPU3	354	4.285	4	1.471	2.165	1	7
IIA1	354	3.528	3	1.629	2.652	1	7
IIA2	354	3.150	3	1.556	2.422	1	7
IIA3	354	3.458	3	1.695	2.872	1	7

A.8 Results for Other Structural Equation Models

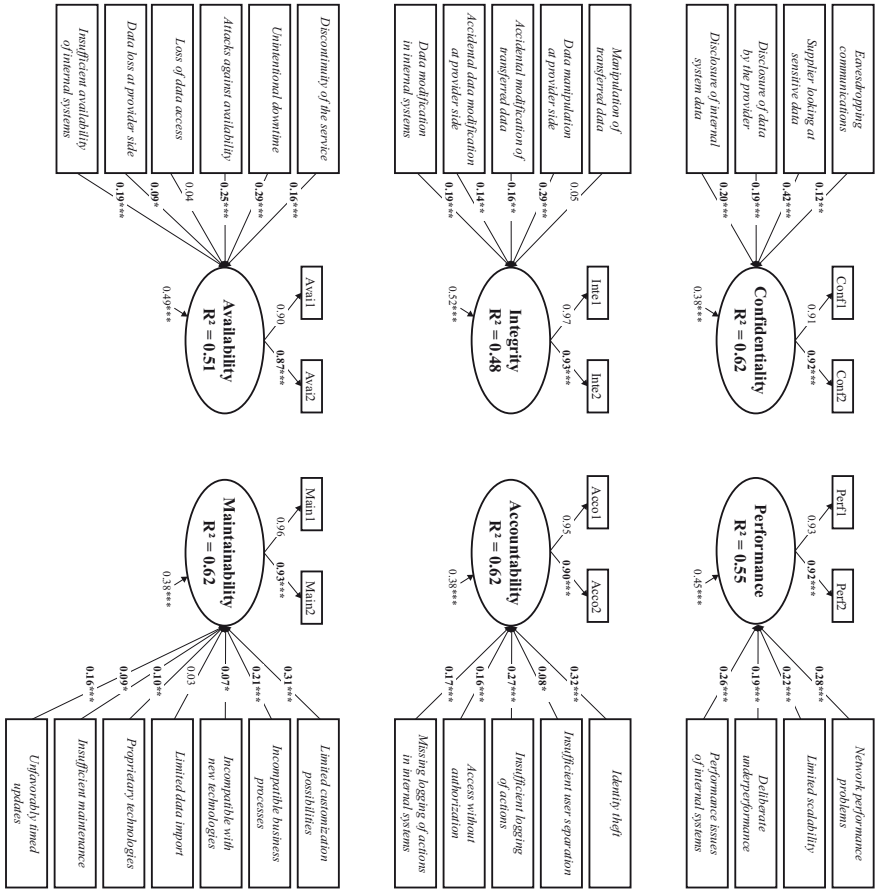


Figure A.8 Results for the Isolated MIMIC Models

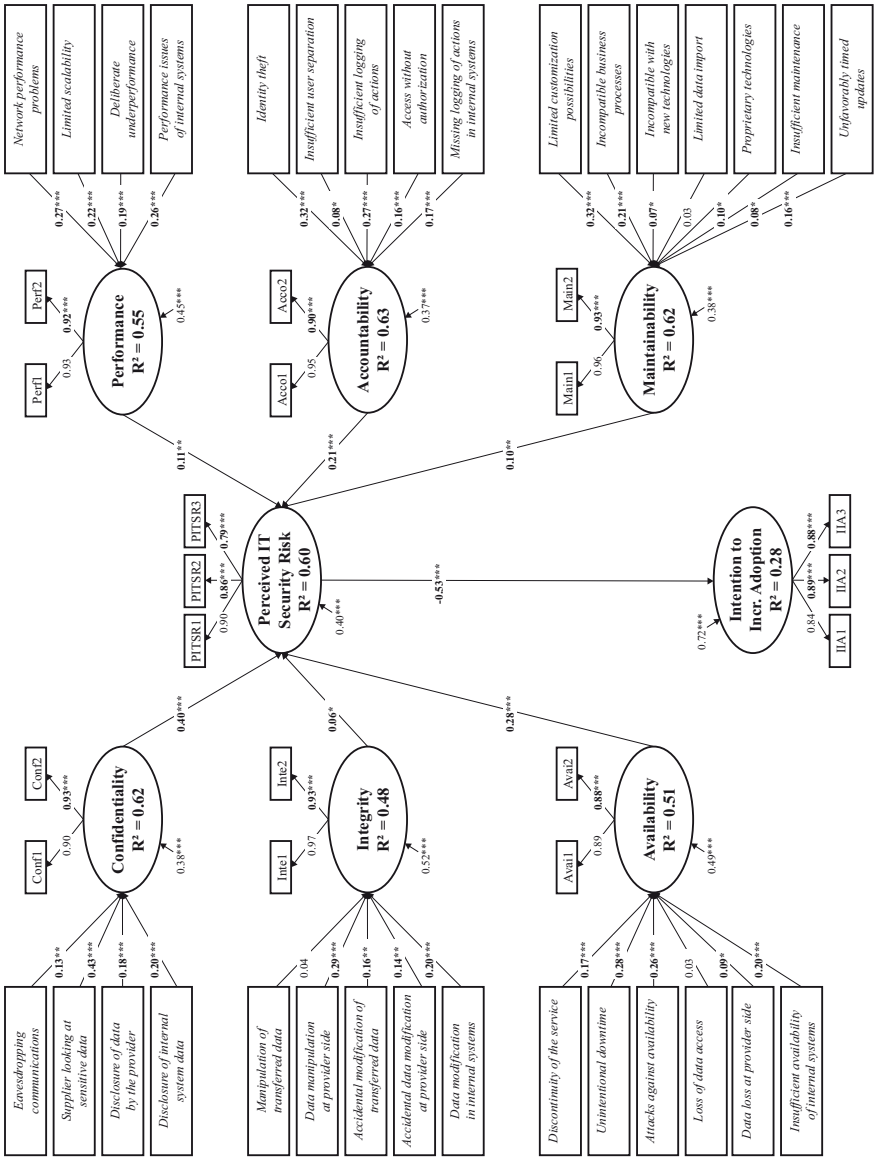


Figure A.9 Results for the Nomological Measurement Model

References

Ackermann T, Buxmann P (2010) Quantifying Risks in Service Networks: Using Probability Distributions for the Evaluation of Optimal Security Levels. In: Proceedings of the 16th Americas Conference on Information Systems (AMCIS 2010), Paper 284

Ackermann T, Miede A, Buxmann P, Steinmetz R (2011) Taxonomy of Technological IT Outsourcing Risks: Support for Risk Identification and Quantification. In: Proceedings of the 19th European Conference on Information Systems (ECIS 2011)

Ackermann T, Widjaja T, Benlian A, Buxmann P (2012) Perceived IT Security Risks of Cloud Computing: Conceptualization and Scale Development. In: Proceedings of the 33rd International Conference on Information Systems (ICIS 2012)

Ackermann T, Widjaja T, Buxmann P (2013) Towards the Optimal Security Level: Quantification of Risks in Service-Based Information Systems. In: Proceedings of the 46th Hawaii International Conference on System Sciences (HICSS 2013)

Ajzen I (1985) From Intentions to Actions: A Theory of Planned Behavior, Springer, Heidelberg, Germany, pp. 11–39

Ajzen I, Fishbein M (1980) Understanding Attitudes and Predicting Social Behavior. Prentice Hall, Englewood Cliffs, NY

Amoroso EG (1994) Fundamentals of Computer Security Technology. Prentice-Hall, Englewood Cliffs, NJ, USA. ISBN 978-0-13-108929-7

Anderson J, Gerbing D (1991) Predicting the Performance of Measures in a Confirmatory Factor Analysis With a Pretest Assessment of Their Substantive Validities. Journal of Applied Psychology 76(5):732–740

Andrews FM (1984) Construct Validity and Error Components of Survey Measures: A Structural Modeling Approach. Public Opinion Quarterly 48(2):409–442

Apte UM, Sobol MG, Hanaoka S, Shimada T, Saarinen T, Salmela T, Vepsalainen APJ (1997) IS Outsourcing Practices in the USA, Japan and Finland: A Comparative Study. Journal of Information Technology 12(4):289–304

Armbrust M, Fox A, Griffith R, Joseph AD, Katz R, Konwinski A, Lee G, Patterson D, Rabkin A, Stoica I, Zaharia M (2010) A View of Cloud Computing. Communications of the ACM 53(4):50–58

Armstrong JS, Overton TS (1977) Estimating Nonresponse Bias in Mail Surveys. Journal of Marketing Research 14(3):396–402

T. Ackermann, *IT Security Risk Management,* DOI 10.1007/978-3-658-01115-4,

© Springer Fachmedien Wiesbaden 2013

Aron R, Clemons EK, Reddi S (2005) Just Right Outsourcing: Understanding and Managing Risk. Journal of Management Information Systems 22(2):37–55

Aubert BA, Rivard S (1998) Assessing the Risk of IT Outsourcing. In: Proceedings of the 31st Annual Hawaii International Conference on System Sciences, pp. 685–692

Aubert BA, Patry M, Rivard S (2005) A Framework for Information Technology Outsourcing Risk Management. The DATA BASE for Advances in Information Systems 36(4):9–28

Avižienis A, Laprie JC, Randell B, Landwehr C (2004) Basic Concepts and Taxonomy of Dependable and Secure Computing. Dependable and Secure Computing, IEEE Transactions on 1(1):11–33

Bagozzi RP (2011) Measurement and Meaning in Information Systems and Organizational Research: Methodological and Philosophical Foundations. MIS Quarterly 35(2):261–292

Bahli B, Rivard S (2003) The information technology outsourcing risk: a transaction cost and agency theory-based perspective. Journal of Information Technology 18(3):211–221

Bahli B, Rivard S (2005) Validating measures of information technology outsourcing risk factors. Omega 33(2):175–187

Bansal G (2011) Security Concerns in the Nomological Network of Trust and Big 5: First Order Vs. Second Order. In: Proceedings of the 32nd International Conference on Information Systems (ICIS), Paper 9

Barki H, Titah R, Boffo C (2007) Information System Use-Related Activity: An Expanded Behavioral Conceptualization of Individual-Level Information System Use. Information Systems Research 18(2):173–192

Baun C, Kunze M, Nimis J, Tai S (2011) Cloud Computing: Web-Based Dynamic IT Services. Springer, New York, NY, USA. ISBN 978-3-642-20917-8

Bedner M, Ackermann T (2010) Schutzziele der IT-Sicherheit. Datenschutz und Datensicherheit (DuD) 34(5):323–328

Beinhauer C, Filiz A (2009) Risikomanagement und Performance Management. Controller Magazin 34(4):85–92

Benefield R (2009) Agile Deployment: Lean Service Management and Deployment Strategies for the SaaS Enterprise. In: 42nd Hawaii International Conference on System Sciences (HICSS), pp. 1–5

Benlian A, Hess T (2010) The Risks of Sourcing Software as a Service: An Empirical Analysis of Adopters and Non-Adopters. In: 18th European Conference on Information Systems (ECIS 2010)

Benlian A, Hess T (2011) Opportunities and risks of software-as-a-service: Findings from a survey of IT executives. Decision Support Systems 52(1):232–246

Benlian A, Hess T, Buxmann P (2009) Drivers of SaaS-Adoption - An Empirical Study of Different Application Types. Business & Information Systems Engineering 1(5):357–369

Bettman JR (1973) Perceived Risk and Its Components: A Model and Empirical Test. Journal of Marketing Research 10(2):184–190

Beulen E, Fenema PV, Currie W (2005) From Application Outsourcing to Infrastructure Management: Extending the Offshore Outsourcing Service Portfolio. European Management Journal 23(2):133–144

Bhattacharya S, Behara RS, Gundersen DE (2003) Business risk perspectives on information systems outsourcing. International Journal of Accounting Information Systems 4(1):75–93

Böhme R, Nowey T (2008) Economic Security Metrics. In: Eusgeld I, Freiling F, Reussner R (eds) Dependability Metrics, Lecture Notes in Computer Science, vol 4909, Springer, Berlin, pp. 176–187

Biskup J (2009) Security in Computing Systems, 1st edn. Springer, Berlin, Germany. ISBN 978-3-540-78441-8

Boehm BW (1981) Software Engineering Economics. Prentice Hall, Upper Saddle River, NJ, USA. ISBN 978-0-13-822122-5

Boehm BW (1991) Software Risk Management: Principles and Practices. IEEE Software 8(1):32–41

Bollen KA (1989) Structural Equations with Latent Variables. John Wiley & Sons, New York

Bollen KA (2011) Evaluating Effect, Composite, and Causal Indicators in Structural Equation Models. MIS Quarterly 35(2):1–14

Bollen KA, Davis WR (2009) Causal Indicator Models: Identification, Estimation, and Testing. Structural Equation Modeling 16(3):498–522

Bolton RN (1993) Pretesting Questionnaires: Content Analyses of Respondents' Concurrent Verbal Protocols. Marketing Science 12(3):280–303

Briscoe G, Marinos A (2009) Digital ecosystems in the clouds: Towards community cloud computing. In: 3rd IEEE International Conference on Digital Ecosystems and Technologies (DEST), pp. 103–108

vom Brocke J, Simons A, Niehaves B, Riemer K, Plattfaut R, Cleven A (2009) Reconstructing the Giant: On the Importance of Rigour in Documenting the Literature Search Process. In: Proceedings of the 17th European Conference on Information Systems (ECIS 2009)

Brooker G (1984) An Assessment of an Expanded Measure of Perceived Risk. Advances in Consumer Research 11(1):439–441

Browne MW, Cudeck R (1993) Alternative Ways of Assessing Model Fit. In: Bollen KA, Long JS (eds) Testing Structural Equation Models, Sage, Newbury Park, CA, USA, pp. 136–162

Brynjolfsson E, Hofmann P, Jordan J (2010) Cloud computing and electricity: beyond the utility model. Communications of the ACM 53(5):32–34

Bundesamt für Sicherheit in der Informationstechnik (BSI) (2010) BSI-Mindestsicherheitsanforderungen an Cloud-Computing-Anbieter. URL http://bit.ly/klanLU

Buxmann P, Ackermann T (2010) IT-Risikomanagement als wirtschaftlicher Erfolgsfaktor. forschen 6(2):12–15

Buxmann P, Hess T, Lehmann S (2008) Software as a Service. Wirtschaftsinformatik 50(6):500–503

Buxmann P, Diefenbach H, Hess T (2011a) Die Softwareindustrie: Ökonomische Prinzipien, Strategien, Perspektiven, 2nd edn. Springer, Heidelberg, Germany. ISBN 978-3-642-13360-2

Buxmann P, Lehmann S, Draisbach T, Koll C, Diefenbach H, Ackermann T (2011b) Cloud Computing und Software as a Service: Konzeption und Preisgestaltung. In: Leible S, Sosnitza O (eds) Online-Recht 2.0: Alte Fragen – neue Antworten?, Boorberg Verlag, Stuttgart, Germany, pp. 21–34

Buyya R, Yeo CS, Venugopal S (2008) Market-Oriented Cloud Computing: Vision, Hype, and Reality for Delivering IT Services as Computing Utilities. In: HPCC '08: Proceedings of the 10th IEEE International Conference on High Performance Computing and Communications 2008, pp. 5–13

Campbell K, Gordon LA, Loeb MP, Zhou L (2003) The economic cost of publicly announced information security breaches: empirical evidence from the stock market. Journal of Computer Security 11(3):431–448

Carmines EG, McIver JP (1981) Analyzing Models with Unobserved Variables. In: Bohrnstedt GW, Borgatta EF (eds) Social Measurement: Current Issues, Sage Publications, Beverly Hills, CA, pp. 65–115

Carr MJ, Konda SL, Monarch I, Ulrich FC, Walker CF (1993) Taxonomy-Based Risk Identification. Technical Report CMU/SEI-93-TR-6, Carnegie Mellon University, Pittsburgh, PA, USA

Casalo L, Flavian C, Guinaliu M (2007) The Impact of Participation in Virtual Brand Communities on Consumer Trust and Loyalty. Online Information Review 31(6):775–792

Cavusoglu H, Mishra B, Raghunathan S (2004a) A model for evaluating IT security investments. Communications of the ACM 47(7):87–92

Cavusoglu H, Mishra B, Raghunathan S (2004b) The Effect of Internet Security Breach Announcements on Market Value: Capital Market Reactions for Breached Firms and Internet Security Developers. International Journal of Electronic Commerce 9(1):70–104

de Chaves SA, Westphall CB, Lamin FR (2010) SLA Perspective in Security Management for Cloud Computing. In: 6th International Conference on Networking and Services (ICNS), pp. 212–217

Chellappa RK, Pavlou PA (2002) Perceived information security, financial liability and consumer trust in electronic commerce transactions. Logistics Information Management 15(5/6):358–368

Churchill GA Jr (1979) A Paradigm for Developing Better Measures of Marketing Constructs. Journal of Marketing Research 16(1):64–73

Chwelos P, Benbasat I, Dexter AS (2001) Research Report: Empirical Test of an EDI Adoption Model. Information Systems Research 12(1):304–321

Cloud Security Alliance (2010) Top Threats to Cloud Computing V1.0. URL http://www.cloudsecurityalliance.org/topthreats

Cloud Security Alliance (2011) Security Guidance for Critical Areas of Focus in Cloud Computing V3.0. URL https://cloudsecurityalliance.org/guidance/csaguide.v3.0.pdf

Combs B, Slovic P (1979) Newspaper Coverage of Causes of Death. Journalism Quarterly 56(4):837–849

Conchar M, Zinkhan G, Peters C, Olavarrieta S (2004) An Integrated Framework for the Conceptualization of Consumers' Perceived-Risk Processing. Journal of the Academy of Marketing Science 32:418–436

Cooper H, Hedges LV, Valentine JC (eds) (2009) The Handbook of Research Synthesis and Meta-Analysis, 2nd edn. Russell Sage Foundation, New York, NY, USA. ISBN 978-0-87154-163-5

Cronbach LJ, Meehl PE (1955) Construct Validity in Psychological Tests. Psychological Bulletin 52(4):281–302

Cunningham SM (1967) The Major Dimensions of Perceived Risk. In: Cox DF (ed) Risk Taking and Information Handling in Consumer Behaviour, Harvard University Press, chap 3, pp. 82–108

Currie WL (2003) A knowledge-based risk assessment framework for evaluating web-enabled application outsourcing projects. International Journal of Project Management 21(3):207–217

Currie WL, Seltsikas P (2001) Delivering Business Critical Information Systems Though Application Service Providers: The Need for a Market Segmentation Strategy. International Journal of Innovation Management 5(3):323–349

Currie WL, Desai B, Khan N (2004) Customer Evaluation of Application Services Provisioning in Five Vertical Sectors. Journal of Information Technology 19(1):39–58

Cusumano MA (2010) Cloud Computing and SaaS as New Computing Platforms. Communications of the ACM 53(4):27–29

Daníelsson J, Jorgensen BN, Samorodnitsky G, Sarma M, de Vries CG (2005) Sub-additivity re-examined: the case for Value-at-Risk. Tech. Rep. 2005-006, EURANDOM

Davis FD (1989) Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology. Management Information Systems Quarterly 13(3):319–339

Dawoud W, Takouna I, Meinel C (2010) Infrastructure as a service security: Challenges and solutions. In: 7th International Conference on Informatics and Systems (INFOS), pp. 1–8

Dübendorfer T, Wagner A, Plattner B (2004) An Economic Damage Model for Large-Scale Internet Attacks. In: Proceedings of the 13th IEEE International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises (WET ICE 2004), pp. 223–228

DeVellis RF (2003) Scale Development, vol 26, 2nd edn. SAGE Publications

Diamantopoulos A (2011) Incorporating Formative Measures into Covariance-Based Structural Equation Models. MIS Quarterly 35(2):335–358

Diamantopoulos A, Siguaw JA (2000) Introducing Lisrel. Sage, London, UK. ISBN 978-0-7619-5171-1

Diamantopoulos A, Winklhofer HM (2001) Index Construction with Formative Indicators: An Alternative to Scale Development. Journal of Marketing Research 38(2):269–277

Diamantopoulos A, Riefler P, Roth KP (2008) Advancing Formative Measurement Models. Journal of Business Research 61(12):1203–1218

Dibbern J (2004) The Sourcing Of Application Software Services: Empirical Evidence Of Cultural, Industry And Functional Differences. Physica-Verlag, Heidelberg, Germany. ISBN 978-3-7908-0217-7

Dibbern J, Goles T, Hirschheim R, Jayatilaka B (2004) Information Systems Outsourcing: A Survey and Analysis of the Literature. The DATA BASE for Advances in Information Systems 35(4):6–102

Duffie D, Pan J (1997) An Overview of Value at Risk. Journal of Derivatives pp. 7–49

Dutta A, Roy R (2008) Dynamics of organizational information security. System Dynamics Review 24(3):349–375

Earl MJ (1996) The risks of outsourcing IT. Sloan Management Review 37(3):26–32

Eckert C (2006) IT-Sicherheit: Konzepte, Verfahren, Protokolle, 4th edn. Oldenbourg Wissenschaftsverlag, München, Germany. ISBN 978-3-486-57851-5

Edwards JR (2001) Multidimensional Constructs in Organizational Behavior Research: An Integrative Analytical Framework. Organizational Research Methods 4(2):144–192

European Network and Information Security Agency (2009) Cloud Computing: Benefits, Risks and Recommendations for Information Security. URL http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-risk-assessment

Everett C (2009) Cloud computing - A question of trust. Computer Fraud & Security 2009(6):5–7

Faisst U, Prokein O (2005) An Optimization Model for the Management of Security Risks in Banking Companies. In: Proceedings of the Seventh IEEE International Conference on E-Commerce Technology (CEC 2005), pp. 266–273

Faisst U, Prokein O, Wegmann N (2007) Ein Modell zur dynamischen Investitionsrechnung von IT-Sicherheitsmaßnahmen. Zeitschrift für Betriebswirtschaft 77(5):511–538

Farahmand F, Atallah M, Konsynski B (2008) Incentives and Perceptions of Information Security Risks. In: Proceedings of the 29th International Conference on Information Systems (ICIS 2008), Paper 25

Featherman MS, Pavlou PA (2003) Predicting e-services adoption: a perceived risk facets perspective. International Journal of Human-Computer Studies 59(4):451–474

Featherman MS, Wells JD (2010) The Intangibility of e-services: Effects on Perceived Risk and Acceptance. The DATA BASE for Advances in Information Systems 41(2):110–131

Featherman MS, Valacich J, Wells JD (2006) Is that Authentic or Artificial? Understanding Consumer Perceptions of Risk in e-Service Encounters. Information Systems Journal 16(2):107–134

Fishbein M, Ajzen I (1975) Belief, Attitude, Intention and Behavior: An Introduction to Theory and Research. Addison-Wesley, Reading, MA

Flavián C, Guinalíu M (2006) Consumer Trust, Perceived Security and Privacy Policy. Industrial Management Data Systems 106(5):601–620

Fornell C, Larcker DF (1981) Evaluating Structural Equation Models with Unobservable Variables and Measurement Error. Journal of Marketing Research 18:39–50

Gefen D, Karahanna E, Straub DW (2003) Trust and Tam in Online Shopping: An Integrated Model. MIS Quarterly 27(1):51–90

Gefen D, Wyss S, Lichtenstein Y (2008) Business Familiarity as Risk Mitigation in Software Development Outsourcing Contracts. MIS Quarterly 32(3):531–542

Gewald H, Dibbern J (2005) The Influential Role of Perceived Risks versus Perceived Benefits in the Acceptance of Business Process Outsourcing: Empirical Evidence from the German Banking Industry. Working Paper 2005-9, E-Finance Lab

Gewald H, Dibbern J (2009) Risks and benefits of business process outsourcing: A study of transaction services in the German banking industry. Information and Management 46(4):249–257

Gewald H, Wüllenweber K, Weitzel T (2006) The influence of perceived risks on banking managers' intention to outsource business processes – a study of the German banking and finance industry. Journal of Electronic Commerce Research 7(2):78–96

Gigerenzer G (2004) Dread Risk, September 11, and Fatal Traffic Accidents. Psychological Science 15(4):286–287

Gonçalves V, Ballon P (2009) An exploratory analysis of Software as a Service and Platform as a Service models for mobile operators. In: 13th International Conference on Intelligence in Next Generation Networks (ICIN), pp. 1–4

Goodman SE, Ramer R (2007) Global Sourcing of IT Services and Information Security: Prudence Before Playing. Communications of AIS 2007(20):812–823

Gordon LA, Loeb MP (2002) The economics of information security investment. ACM Transactions on Information and Systems Security 5(4):438–457

Gouscos D, Kalikakis M, Georgiadis P (2003) An Approach to Modeling Web Service QoS and Provision Price. In: Proceedings of the Fourth International Conference on Web Information Systems Engineering Workshops (WISEW 2003), pp. 121–130

Gregory R, Mendelsohn R (1993) Perceived Risk, Dread, and Benefits. Risk Analysis 13(3):259–264

Hahn ED, Doh J, Bunyaratavej K (2009) The Evolution of Risk in Information Systems Offshoring: The Impact of Home Country Risk, Firm Learning, and Competitive Dynamics. Management Information Systems Quarterly 33(3):597–616

Hansen L (2005) Opportunities, Threats and Critical Success Factors of the ASP Business Model. In: eChallenges e-2004

Harrison DA, Mykytyn Jr PP, Riemenschneider CK (1997) Executive Decisions About Adoption of Information Technology in Small Business: Theory and Empirical Tests. Information Systems Research 8(2):171–195

Havlena WJ, DeSarbo WS (1990) On the Measurement of Perceived Consumer Risk. Decision Sciences 22:927–939

Herath H, Herath T (2008) Investments in Information Security: A Real Options Perspective with Bayesian Postaudit. Journal of Management Information Systems 25(3):337–375

Hilkert D, Benlian A, Sarstedt M, Hess T (2011) Perceived Software Platform Openness: The Scale and its Impact on Developer Satisfaction. In: Proceedings of the 32nd International Conference on Information Systems (ICIS 2011), Paper 13

Hinkin TR (1998) A Brief Tutorial on the Development of Measures for Use in Survey Questionnaires. Organizational Research Methods 1(1):104–121

Hirschheim R, Lacity MC (2000) The Myths and Realities of Information Technology Insourcing. Communications of the ACM 43(2):99–107

Homburg C, Giering A (1996) Konzeptualisierung und Operationalisierung komplexer Konstrukte. Marketing – Zeitschrift für Forschung und Praxis 18(1):5–24

Howard JD, Longstaff TA (1998) A Common Language for Computer Security Incidents. Technical Report SAND98-8667, Sandia National Laboratories, Albuquerque, NM, USA

Howard RA (1988) Decision Analysis: Practice and Promise. Management Science 34(6):679–695

Hu Lt, Bentler PM (1999) Cutoff Criteria for Fit Indexes in Covariance Structure Analysis: Conventional Criteria Versus New Alternatives. Structural Equation Modeling 6(1):1–55

Itani W, Kayssi A, Chehab A (2009) Privacy as a Service: Privacy-Aware Data Storage and Processing in Cloud Computing Architectures. In: 8th IEEE International Conference on Dependable, Autonomic and Secure Computing (DASC), pp. 711–716

Jarvis CB, MacKenzie SB, Podsakoff PM (2003) A Critical Review of Construct Indicators and Measurement Model Misspecification in Marketing and Consumer Redearch. Journal of Consumer Research 30(2):199–218

Jayatilaka B, Schwarz A, Hirschheim R (2003) Determinants of ASP Choice: An Integrated Perspective. European Journal of Information Systems 12(3):210–224

Jensen M, Schwenk J, Gruschka N, Iacono LL (2009) On Technical Security Issues in Cloud Computing. In: IEEE International Conference on Cloud Computing (CLOUD), pp. 109–116

Jorion P (2006) Value at Risk: The New Benchmark for Managing Financial Risk, 3rd edn. McGraw-Hill, New York, NY, USA. ISBN 978-0-07-146495-6

Jöreskog KG, Sörbom D (2006) Lisrel 8.80. Chicago: Scientific Software International

Jurison J (1995) The Role of Risk and Return in Information Technology Outsourcing Decisions. Journal of Information Technology 10(4):239–247

Kaufman LM (2009) Data Security in the World of Cloud Computing. IEEE Security Privacy 7(4):61–64

Kern T, Kreijger J, Willcocks L (2002a) Exploring ASP as sourcing strategy: theoretical perspectives, propositions for practice. The Journal of Strategic Information Systems 11(2):153–177

Kern T, Lacity MC, Willcocks LP (2002b) Netsourcing: Renting Business Applications and Services Over a Network, 1st edn. Financial Times Prentice Hall Books, Pearson Education, Upper Saddle River, NJ, USA. ISBN 978-0-13-092355-4

Kern T, Willcocks LP, Lacity MC (2002c) Application service provision: risk assessment and mitigation. MIS Quarterly Executive 1(2):113–126

van Kessel P (2009) Outpacing change: Ernst & Young's 12th annual global information security survey

Kim DJ, Ferrin DL, Rao HR (2008) A Trust-based Consumer Decision-making Model in Electronic Commerce: The Role of Trust, Perceived Risk, and their Antecedents. Decision Support Systems 44(2):544–564

Koller M (1988) Risk as a Determinant of Trust. Basic and Applied Social Psychology 9(4):265–276

Lacity MC, Willcocks LP, Feeny DF (1995) IT Outsourcing: Maximize Flexibility and Control. Harvard Business Review 73(3):84–93

Lacity MC, Khan SA, Willcocks LP (2009) A review of the IT outsourcing literature: Insights for practice. The Journal of Strategic Information Systems 18(3):130–146

Lacity MC, Khan S, Yan A, Willcocks LP (2010) A Review of the IT Outsourcing Empirical Literature and Future Research Directions. Journal of Information Technology 25(4):395–433

Landwehr CE (2001) Computer Security. International Journal of Information Security 1(1):3–13

Law AM, Kelton WD (2000) Simulation Modeling and Analysis, 3rd edn. Mc Graw-Hill, Singapore. ISBN 978-0-07-059292-6

Lehmann S, Buxmann P (2009) Preisstrategien von Softwareanbietern. Wirtschaftsinformatik 51(6):519–529

Lenk A, Klems M, Nimis J, Tai S, Sandholm T (2009) What's inside the Cloud? An architectural map of the Cloud landscape. In: International Conference on Software Engineering Proceedings of the 2009 ICSE Workshop on Software Engineering Challenges of Cloud Computing, pp. 23–31

Levy Y, Ellis TJ (2006) A Systems Approach to Conduct an Effective Literature Review in Support of Information Systems Research. Informing Science Journal 9:181–212

Loh L, Venkatraman N (1995) An Empirical Study of Information Technology Outsourcing: Benefits, Risks, and Performance Implications. In: Proceedings of the 16th International Conference on Information Systems (ICIS), Paper 25

Lu Y, Sun B (2009) The Fitness Evaluation Model of SAAS for Enterprise Information System. In: IEEE International Conference on e-Business Engineering (ICEBE), pp. 507–511

Luo X, Li H, Zhang J, Shim JP (2010) Examining Multi-Dimensional Trust and Multi-Faceted Risk in Initial Acceptance of Emerging Technologies: An Empirical Study of Mobile Banking Services. Decision Support Systems 49(2):222–234

Álvarez G, Petrović S (2003) A new taxonomy of Web attacks suitable for efficient encoding. Computers & Security 22(5):435–449

Ma Q, Pearson JM, Tadisina S (2005) An exploratory study into factors of service quality for application service providers. Information and Management 42(8):1067–1080

MacCallum RC, Browne MW (1993) The Use of Causal Indicators in Covariance Structure Models: Some Practical Issues. Psychological Bulletin 114(3):533–541

Machina MJ (1987) Decision-Making in the Presence of Risk. Science 236:537–543

MacKenzie SB, Podsakoff PM, Podsakoff NP (2011) Construct Measurement and Validation Procedures in MIS and Behavioral Research: Integrating New and Existing Techniques. MIS Quarterly 35(2):293–334

March JG, Shapira Z (1987) Managerial Perspectives on Risk and Risk Taking. Management Science 33(11):1404–1418

Marston S, Li Z, Bandyopadhyay S, Zhang J, Ghalsasi A (2011) Cloud Computing: The Business Perspective. Decision Support Systems 51(1):176–189

Mather T, Kumaraswamy S, Latif S (2009) Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance, 1st edn. O'Reilly Media, Sebastopol, CA, USA. ISBN 978-0-596-80276-9

McNeil AJ, Frey R, Embrechts P (2005) Quantitative Risk Management: Concepts, Techniques, Tools, 1st edn. Princeton University Press, Princeton, NJ, USA. ISBN 978-0-691-12255-7

Mell P, Grance T (2011) The NIST Definition of Cloud Computing. Special Publication 800-145, National Institute of Standards and Technology

Miede A, Ackermann T, Repp N, Abawi DF, Steinmetz R, Buxmann P (2010a) Attacks on the Internet of Services: The Security Impact of Cross-organizational Service-based Collaboration. In: Schumann M, Kolbe LM, Breitner MH, Frerichs A (eds) Tagungsband Multikonferenz Wirtschaftsinformatik (MKWI 2010), pp. 2151–2162

Miede A, Nedyalkov N, Gottron C, König A, Repp N, Steinmetz R (2010b) A Generic Metamodel for IT Security – Attack Modeling for Distributed Systems. In: Proceedings of the Fifth International Conference on Availability, Reliability, and Security (ARES 2010), pp. 430–437

Minutoli G, Fazio M, Paone M, Puliafito A (2009) Virtual business networks with Cloud Computing and virtual machines. In: International Conference on Ultra Modern Telecommunications Workshops (ICUMT), pp. 1–6

Mitchell VW, Greatorex M (1993) Risk Perception and Reduction in the Purchase of Consumer Services. The Service Industries Journal 13:179–200

Mitschele A (2008) Intelligente Methoden im Integrierten Risikomanagement. Dissertation, Universität Karlsruhe (TH), Fakultät für Wirtschaftswissenschaften, Institut für Angewandte Informatik und Formale Beschreibungsverfahren (AIFB)

Moore GC, Benbasat I (1991) Development of an Instrument to Measure the Perceptions of Adopting an Information Technology Innovation. Information Systems Research 2(3):192–222

Mowbray M, Pearson S (2009) A client-based privacy manager for cloud computing. In: 4th International ICST Conference on COMmunication System softWAre and middlewaRE (COMSWARE), pp. 1–8

Mullender S (1993) Distributed Systems, 2nd edn. ACM Press, New York, NY, USA. ISBN 978-0-201-62427-4

Nahm AY, Solís-Galván LE, Rao SS, Ragu-Nathan TS (2002) The Q-sort Method: Assessing Reliability and Construct Validity of Questionnaire Items at a Pre-Testing Stage. Journal of Modern Applied Statistical Methods 1(1):114–125

Nakatsu RT, Iacovou CL (2009) A comparative study of important risk factors involved in offshore and domestic outsourcing of software development projects: A two-panel Delphi study. Information & Management 46(1):57–68

Nunnally J, Bernstein I (1994) Psychometric Theory, 3rd edn. McGraw-Hill, New York, NY, USA. ISBN 978-0-07-047849-7

Olovsson T (1992) A Structured Approach to Computer Security. Technical Report 122, Chalmers University of Technology

Osei-Bryson KM, Ngwenyama OK (2006) Managing risks in information systems outsourcing: An approach to analyzing outsourcing risks and structuring incentive contracts. European Journal of Operational Research 174(1):245–264

Pang G, Whitt W (2009) Service Interruptions in Large-Scale Service Systems. Management Science 55(9):1499–1512

Patnayakuni R, Seth N (2001) Why license when you can rent? Risks and rewards of the application service provider model. In: ACM SIGCPR Conference on Computer Personnel Research (SIGCPR), pp. 182–188

Patterson DA (2002) A Simple Way to Estimate the Cost of Downtime. In: Proceedings of the 16th USENIX Conference on System Administration (LISA 2002), pp. 185–188

Pavlou PA, Liang H, Xue Y (2007) Understanding and Mitigating Uncertainty in Online Exchange Relationships: A Principal-Agent Perspective. Management Information Systems Quarterly 31(1):105–136

Peter JP, Ryan MJ (1976) An investigation of perceived risk at the brand level. Journal of Marketing Research 13(2):184–188

Peter JP, Tarpey LX Sr (1975) A comparative analysis of three consumer decision strategies. Journal of Consumer Research 2:29–37

Petter S, Straub DW, Rai A (2007) Specifying Formative Constructs In Information Systems Research. MIS Quarterly 31(4):623–656

Phillips LW (1981) Assessing Measurement Error in Key Informant Reports: A Methodological Note on Organizational Analysis in Marketing. Journal of Marketing Research 18(4):395–415

Pinto CA, Arora A, Hall D, Schmitz E (2006) Challenges to Sustainable Risk Management: Case Example in Information Network Security. Engineering Management Journal 18(1):17–24

Podsakoff PM, Organ DW (1986) Self-Reports in Organizational Research: Problems and Prospects. Journal of Management 12(4):531–544

Polites GL, Roberts N, Thatcher J (2012) Conceptualizing Models Using Multidimensional Constructs: A Review and Guidelines for their Use. European Journal of Information Systems 21:22–48

Ponemon L (2009) Fourth Annual US Cost of Data Breach Study: Benchmark Study of Companies

Poppo L, Zenger T (2002) Do Formal Contracts and Relational Governance Function as Substitutes or Complements? Strategic Management Journal 23:707–725

Pring B (2010) Cloud Computing: The Next Generation of Outsourcing. Tech. Rep. G00207255, Gartner

Pring B, Brown RH, Leong L, Couture AW, Biscotti F, Lheureux BJ, Frank A, Roster J, Cournoyer S, Liu VK (2010) Forecast: Public Cloud Services, Worldwide and Regions, Industry Sectors, 2009–2014. Tech. Rep. G00200833, Gartner

Prokein O (2008) IT-Risikomanagement: Identifikation, Quantifizierung und wirtschaftliche Steuerung. Gabler, Wiesbaden, Germany. ISBN 978-3-8349-0870-4

Quinn JB, Hilmer FG (1994) Strategic Outsourcing. Sloan Management Review 35(4):43–55

Rhee HS, Ryu YU, Kim CT (2012) Unrealistic Optimism on Information Security Management. Computers & Security 31(2):221–232

Richardson R (2009) CSI Computer Crime and Security Survey 2009

Roßnagel A, Pfitzmann A, Garstka H (2001) Modernisierung des Datenschutzrechts. Gutachten im Auftrag des Bundesministeriums des Innern, URL http://www.lda.brandenburg.de/sixcms/media.php/2473/dsmodern.pdf

Ross SM (1996) Stochastic Processes, 2nd edn. John Wiley & Sons, New York, NY, USA. ISBN 978-0-471-12062-9

Sang J, Rego V, Spragins J (1992) Efficient Algorithms for Joint Density Approximations of Discrete Independent Random Variables. Technical Report CSD-TR-92-085, Purdue University, West Lafayette, IN, USA

Söbbing T (2006) Handbuch IT-Outsourcing: Recht, Strategie, Prozesse, IT, Steuern samt Business Process Outsourcing, 3rd edn. C. F. Müller, Heidelberg, Germany. ISBN 978-3-8114-3320-5

Schlaak B, Dynes S, Kolbe LM, Schierholz R (2008) Managing of Information Systems Risks in Extended Enterprises: The Case of Outsourcing. In: Proceedings of the 14th Americas Conference on Information Systems (AMCIS 2008), Paper 280

Schneier B (2004) Secrets and Lies: Digital Security in a Networked World. John Wiley & Sons, New York, NY, USA. ISBN 978-0-471-45380-2

Schwarz A, Jayatilaka B, Hirschheim R, Goles T (2009) A Conjoint Approach to Understanding IT Application Services Outsourcing. Journal of the AIS 10(10):748–781

Simon HA (1960) The New Science of Management Decision, 1st edn. Harper & Row, New York, NY, USA. ISBN 978-0-13-616136-3

Sjöberg L, Engelberg E (2010) Risk Perception and Movies: A Study of Availability as a Factor in Risk Perception. Risk Analysis 30(1):95–106

Slovic P (1987) Perception of risk. Science 236(4799):280–285

Smart NP, Vercauteren F (2010) Fully Homomorphic Encryption with Relatively Small Key and Ciphertext Sizes. In: Nguyen P, Pointcheval D (eds) Public Key Cryptography – PKC 2010, Lecture Notes in Computer Science, vol 6056, Springer Berlin / Heidelberg, Germany, pp. 420–443

Smith GF (1992) Towards a Theory of Managerial Problem Solving. Decision Support Systems 8(1):29–40

Sommerville I (2006) Software Engineering, 8th edn. Pearson/Addison-Wesley, Harlow, Essex, UK. ISBN 978-0-321-31379-9

Sonnenreich W, Albanese J, Stout B (2006) Return On Security Investment (ROSI): A Practical Quantitative Model. Journal of Research and Practice in Information Technology 38(1):45–56

Soo Hoo KJ (2000) How much is enough: a risk management approach to computer security. PhD thesis, Stanford University, Stanford, CA, USA

Stelzer D (1993) Sicherheitsstrategien in der Informationsverarbeitung. Deutscher Universitäts Verlag, Wiesbaden, Germany. ISBN 978-3-8244-2038-4

Stewart KA, Segars AH (2002) An Empirical Examination of the Concern for Information Privacy Instrument. Infor 13(1):36–49

Straub DW, Boudreau MC, Gefen D (2004) Validation Guidelines for IS Positivist Research. Communications of the Association for Information Systems 13:Article 24

Streitberger W, Ruppel A (2009) Cloud Computing Sicherheit: Schutzziele. Taxonomie. Marktübersicht. Fraunhofer-Institut für Sichere Informationstechnologie (SIT), Garching, Germany. ISBN 978-3-9813317-0-7

Swartz N (2004) Offshoring Privacy. Information Management Journal 38(5):24–26

Tchankova L (2002) Risk Identification: Basic Stage in Risk Management. Environmental Management and Health 13(3):290–297

The Open Web Application Security Project (OWASP) (2010) OWASP Top 10 – 2010: The Ten Most Critical Web Application Security Risks. URL http://bit.ly/bFax6s

Tversky A, Kahneman D (1973) Availability: A heuristic for judging frequency and probability. Cognitive Psychology 4:207–232

Valacich JS, Sarker S, Pratt J, Groomer M (2009) Understanding Risk-Taking Behavior of Groups: A "Decision Analysis" Perspective. Decision Support Systems 46(4):902–912

Vaquero LM, Rodero-Merino L, Caceres J, Lindner M (2009) A Break in the Clouds: Towards a Cloud Definition. ACM SIGCOMM Computer Communication Review 39(1):50–55

Vaquero LM, Rodero-Merino L, Morán D (2011) Locking the Sky: A Survey on IaaS Cloud Security. Computing 91:93–118

Venkatesh V, Morris MG, Davis GB, Davis FD (2003) User Acceptance of Information Technology: Toward a Unified View. Management Information Systems Quarterly 27(3):425–478

Viega J (2009) Cloud Computing and the Common Man. Computer 42(8):106–108

Vitharana P, Dharwadkar R (2007) Information Systems Outsourcing: Linking Transaction Cost and Institutional Theories. Communications of the AIS 2007(20):346–370

Walsh KR (2003) Analyzing the Application ASP Concept: Technologies, Economies, and Strategies. Communications of the ACM 46(8):103–107

Wang C, Wang Q, Ren K, Lou W (2009) Ensuring Data Storage Security in Cloud Computing. Cryptology ePrint Archive, Report 2009/081, URL http://eprint.iacr.org/2009/081

Wang J, Chaudhury A, Rao HR (2008) A Value-at-Risk Approach to Information Security Investment. Information Systems Research 19(1):106–120, http://isr.journal.informs.org/cgi/reprint/19/1/106.pdf

Weiber R, Mühlhaus D (2009) Strukturgleichungsmodellierung. Springer, Germany

Weinhardt C, Anandasivam A, Blau B, Borissov N, Meinl T, Michalk W, Stößer J (2009) Cloud Computing: A Classification, Business Models, and Research Directions. Business & Information Systems Engineering 1(5):391–399

West DHD (1979) Updating Mean and Variance Estimates: An Improved Method. Communications of the ACM 22(9):532–535

Wheaton B, Muthen B, Alwin DF, Summers GF (1977) Assessing Reliability and Stability in Panel Models. Sociological Methodology 8(1):84–136

Wheeler E (2011) Security Risk Management: Building an Information Security Risk Management Program from the Ground Up, 1st edn. Elsevier, Amsterdam, Netherlands. ISBN 978-1-59749-615-5

Whitten D, Wakefield RL (2006) Measuring Switching Costs in IT Outsourcing Services. The Journal of Strategic Information Systems 15(3):219–248

Willcocks L, Lacity MC, Cullen S (2007) Information Technology Sourcing Research: Critique, Lessons and Prospects. In: Proceedings of the 13th Americas Conference on Information Systems (AMCIS 2007), Paper 359

Willcocks LP, Fitzgerald G, Lacity MC (1996) To outsource IT or not? Recent Research on Economics and Evaluation Practice. European Journal of Information Systems 5(3):143–160

Wolke T (2008) Risikomanagement, vol 2. Oldenbourg, München, Germany. ISBN 978-3-486-58714-2

Xia W, Lee G (2005) Complexity of Information Systems Development Projects: Conceptualization and Measurement Development. Journal of Management Information Systems 22(1):45–83

Yildiz M, Abawajy J, Ercan T, Bernoth A (2009) A Layered Security Approach for Cloud Computing Infrastructure. In: 10th International Symposium on Pervasive Systems, Algorithms, and Networks (ISPAN), pp. 763–767

Ying W, Li A, Xu L (2008) Research on the authentication strategy of ASP mode-based networked manufacturing system. In: IEEE/ASME International Conference on Advanced Intelligent Mechatronics (AIM), pp. 1014–1017

Zhang X, Schiffman J, Gibbs S, Kunjithapatham A, Jeong S (2009) Securing elastic applications on mobile devices for cloud computing. In: ACM workshop on Cloud Computing Security (CCSW), pp. 127–134

Zhou L, Liu D, Wang B (2008) Research on ASP-Based Information Security System. In: International Symposium on Computer Science and Computational Technology (ISCSCT), pp. 746–749

Some parts, ideas, and figures will appear in the following, currently unpublished articles:

Ackermann T, Widjaja T, Benlian A, Buxmann P. The Nature and Dual Inhibitory Role of IT Security Risks in Cloud Adoption – Insights from a Mixed-Methods Study. *Under review*

Ackermann T, Widjaja T, Benlian A, Buxmann P. Perceived IT Security Risks of Cloud Computing: Conceptualization and Scale Development. *To be submitted*