# IT Security Risk Management of Cloud Computing Services in Critical Infrastructures

Inauguraldissertation
zur Erlangung des akademischen Grades eines Doktors
der Wirtschaftswissenschaften des Fachbereichs Wirtschaftswissenschaften
der Universität Osnabrück

vorgelegt von

Michael Adelmeyer, M. Sc.

Osnabrück, September 2019

**Dekanin**
Prof. Dr. Valeriya Dinger

**Referenten**
Prof. Dr. Frank Teuteberg
Prof. Dr. Oliver Thomas

**Datum der Disputation**
11. September 2019

# Preface

This cumulative dissertation was prepared between November 2015 and January 2019 during my work as a research assistant at the Institute of Accounting and Information Systems of the School of Business Administration and Economics at Osnabrück University.

I would like to take this opportunity to express my sincere gratitude to my supervisor, Prof. Dr. Frank Teuteberg, for his continuous support and invaluable feedback on my research. I am gratefully indebted to him for his constructive and unstinting guidance.

In addition, I would like to acknowledge Prof. Dr. Oliver Thomas as co-advisor of this thesis.

Particularly, I would like to thank Dr. Marc Walterbusch, who supervised my master’s thesis and fostered my interest in the present topic. Further, he provided me with valuable insights and seasoned suggestions from his former work as a research assistant at the Institute of Accounting and Information Systems.

I would like to express my appreciation to the team of the institute, in particular Mrs. Marita Imhorst, Mr. Jan Heinrich Beinke, Mr. Christian Fitte and Mr. Pascal Meier, whose constructive feedback and corrections greatly contributed to the dissertation project.

Furthermore, I would like to thank the co-authors of the publications contained in this cumulative dissertation, namely (in alphabetical order), Mr. Lukas Beike, Mr. Jan Heinrich Beinke, Mr. Peter Biermanski, Mr. Mirko Buggenthin, Mr. Ricardo Ramos Gameiro, Mr. Michael Goldshteyn, Prof. Dr. Peter König, Mr. Julian Lang, Mr. Pascal Meier, Mr. Sebastian Osada, Mr. Christopher Petrick, Mr. Kai Seifert and Dr. Marc Walterbusch, for their valuable and manifold contributions.

I would also like to thank my family and friends, who have reminded me in recent years of the pleasures beyond the doctoral thesis. A special thanks is addressed to my parents, Carla and Matthias Adelmeyer, who have supported me in every possible way in my life so far.

Finally, I would like to express my utmost gratitude to my loving fiancée Anna Maria Wehming, who has always encouraged and supported me unreservedly in this project from the very beginning. I would like to thank her for her understanding motivation and assistance and for believing in me and my capabilities.

Osnabrück, September 2019 Michael Adelmeyer

# Notes on the Structure of the Document

This cumulative dissertation is structured in two parts:

Part A provides an introductory overview of the relevant research contributions. Based on the motivation of the research project, the underlying research design is explained. Afterwards, in a summary of the results, the included research contributions are placed in the overall context of this cumulative dissertation. Subsequently, implications for research and practice, limitations of the work, and potential starting points for future research are discussed. Part A closes with a conclusion and can therefore be regarded as a stand-alone document with separate listings of abbreviations, figures and tables at the beginning and cited references at the end.

Part B contains the research contributions and their appendices that are included in Part A of this cumulative dissertation. Where possible, the formatting of the individual contributions and the citation styles are retained based on the different specifications of the respective publication organs. The references within the articles contained in Part B refer to the bibliography of the respective articles.

# Contents

# Part A: Introductory Overview

# List of Abbreviations

| | |
|---|---|
| AJAX | Asynchronous JavaScript and XML |
| AO | Abgabenordnung |
| AtG | Atomgesetz |
| B3S | Branchenspezifische Sicherheitsstandards |
| BDSG | Bundesdatenschutzgesetz |
| BSI | Bundesamt für Sicherheit in der Informationstechnik |
| BSIG | Gesetz über das Bundesamt für Sicherheit in der Informationstechnik |
| CI | Critical Infrastructure |
| CMF | Content Management Framework |
| CMS | Content Management System |
| CO | Comprehension |
| COBIT | Control Objectives for Information and Related Technology |
| COSO | Committee of Sponsoring Organizations of the Treadway Commission |
| CSA | Cloud Security Alliance |
| CSS | Cascading Style Sheets |
| CTRL | (perceived) Control |
| DFT | Direct Functional Trust |
| EC | European Commission |
| EnWG | Energiewirtschaftsgesetz |
| EOU | Ease of Use |
| ERM | Enterprise Risk Management |
| FAIT | Fachausschuss Informationstechnologie |
| GDPR | General Data Protection Regulation |
| HGB | Handelsgesetzbuch |
| HTML | Hypertext Markup Language |
| HTTP | Hypertext Transfer Protocol |
| IaaS | Infrastructure as a Service |
| IDW | Institut der Wirtschaftsprüfer |
| IEC | International Electrotechnical Commission |
| IFT | Indirect Functional Trust |
| IO | (perceived) Information Overload |
| ISAE | International Standards for Assurance Engagements |
| ISMS | Information Security Management System |
| ISO | International Organization for Standardization |
| IT | Information Technology |
| ITIL | Information Technology Infrastructure Library |
| ITU | Intention to Use |
| ITUM | Intention to Use a Mediator |
| ITUP | Intention to Use a Provider |
| JSON | JavaScript Object Notation |
| KPI | Key Performance Indicator |
| KritisV | Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSIG |
| NIST | National Institute of Standards and Technology |
| PaaS | Platform as a Service |
| PHP | PHP: Hypertext Preprocessor |
| PHR | Personal Health Record |
| PLS | Partial Least Squares |

| | |
|---|---|
| PRI | (perceived) Privacy |
| PS | Prüfungsstandard |
| RECC | Rebound Effect in Cloud Computing |
| RQ | Research Question |
| RT | Referral Trust |
| SaaS | Software as a Service |
| SEC | (perceived) Security |
| SEM | Structural Equation Model |
| SLA | Service Level Agreement |
| SOC | Service Organization Control |
| SSAE | Statement on Standards for Attestation Engagements |
| TB | Trusting Beliefs |
| TKG | Telekommunikationsgesetz |
| TMG | Telemediengesetz |
| TR | Trust |
| TRA | Transparency |
| VHB | Verband der Hochschullehrer für Betriebswirtschaftslehre |
| WKWI | Wissenschaftliche Kommission Wirtschaftsinformatik |
| WPO | Wirtschaftsprüferordnung |
| XML | Extensible Markup Language |

# List of Figures

# List of Tables

# 1 Introduction

## 1.1 Motivation and Background

Due to the considerable advantages of cloud computing, such as cost efficiency, flexibility, and scalability (Armbrust et al. 2010; Marston et al. 2011), the technology pervades the IT industry and has transformed the means of IT service provisioning (Kushida et al. 2011). Cloud computing can be defined as a model for ubiquitous network access to a shared pool of configurable computing resources (e.g., network, servers, storage, applications, and services) that can be rapidly provisioned on-demand in a self-service model requiring minimal management or service provider interaction (Mell and Grance 2011). Cloud computing relies on three core technologies, namely, virtualization, multitenancy, and web services (Marston et al. 2011). Regarding the type of the provisioned service, different service models are distinguished. Infrastructure as a Service (IaaS) describes the provision of fundamental computing resources over a network, based on which a customer is able to deploy his own services. In Platform as a Service (PaaS) environments, self-developed or acquired applications can be run. Software as a Service (SaaS) refers to online applications that are provided over the network (Mell and Grance 2011). Irrespective of the service model in use, the user does not manage or control the underlying cloud infrastructure (Mell and Grance 2011). Regarding the range of potential users, multiple deployment models (private, public, community, and hybrid) can be differentiated. In private clouds, the cloud infrastructure is exclusively provisioned and used by a single organization. In contrast, public clouds are open to the general public. In community clouds, services are provided solely for a specific community of users with shared concerns or interests. Hybrid clouds are compositions of multiple distinct cloud infrastructures (Mell and Grance 2011).

To realize the proclaimed benefits of the technology, critical infrastructure (CI) providers increasingly deploy (high-assurance) IT services, processes, and functions in cloud environments (Bless et al. 2013; Diez and Silva 2011; Hecht et al. 2014; Schöller et al. 2013; Wagner et al. 2015). The European Council defines a critical infrastructure as *"an asset, system or part thereof located in Member States which is essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which would have a significant impact in a Member State as a result of the failure to maintain those functions"* (European Council 2008). The identification of CIs and the definition of the corresponding thresholds, criteria, and sectors are subject to national directives, protection plans, and policy frameworks (Yusta et al. 2011). For example, the German law to increase the safety of information technology systems (IT-Sicherheitsgesetz, translated *"IT Security Law"*), which became effective in July 2015, distinguishes seven different CI sectors, namely, energy, information and telecommunication, transport and traffic, healthcare, water, food, and finance and insurance. Since information technology commonly forms the backbone of CIs, the resilience and security of their IT systems is of crucial importance for reliable operation (Ten and Manimaran 2010). Thus, the IT Security Law requires CI providers of the aforementioned sectors to protect and secure their IT against cyberattacks. Cloud providers as "digital service providers" are further directly committed to ensure a certain level of IT security (Adelmeyer, Petrick, et al. 2018).

Since the control over the underlying cloud infrastructure and the corresponding security measures is delegated to the cloud provider (Mell and Grance 2011; Zissis and Lekkas 2012), the outsourcing of systems, data or functions to cloud environments exposes CIs to security risks and leads to additional security challenges (Paudel et al. 2014; Rudolph et al. 2014). The loss of control and the corresponding dependency further requires trust in the security measures of the respective cloud service providers (Zissis and Lekkas 2012). This is especially crucial since CIs highly rely on IT systems for dependable service provisioning (Ten and Manimaran 2010). Therefore, the IT landscapes and corresponding cloud deployments of CIs are subject to high protection requirements and legislation regarding security, privacy, and resilience, which differ in comparison to those of industrial actors (Bless et al. 2013; Hecht et al. 2014). Furthermore, when adopting cloud services in CIs, the manifold security demands of various stakeholders have to be taken into account (Rudolph et al. 2014). However, due to the opacity of and the control delegation in cloud environments, the specific risks, threats, and vulnerabilities for CIs resulting from outsourcing into cloud environments are difficult to assess (Hecht et al. 2014). In addition, each cloud deployment is afflicted with individual risks depending on the selected cloud service and deployment model (Pearson 2013; Weintraub and Cohen 2016; Zissis and Lekkas 2012). Furthermore, standards and statutory regulations strongly influence security requirements and in consequence the corresponding management of cloud-related risks (Baldwin et al. 2013).

The virtualization and sourcing of resources via clouds require individual approaches for identifying risks and determining measures to achieve acceptable residual risks for both service providers and customers (Adelmeyer, Petrick, et al. 2018; Königs 2017). Due to the storage and processing of data at external providers, most traditional IT risk management methods cannot be directly adapted to cloud environments (Ackermann 2013; Damenu and Balakrishna 2015), which results in the need for new risk management approaches for the effectiveness of security controls and measures (Drissi et al. 2013) on the parts of both users and cloud service providers (Baldwin et al. 2013). IT security risks, which primarily threaten the confidentiality, integrity, and availability of systems and data in clouds (Adelmeyer, Walterbusch, Lang, et al. 2017; Eckert 2018), are regarded as the most salient risks associated with cloud services (Ackermann 2013). Due to the strict requirements regarding the IT security of their landscapes (Bless et al. 2013; Hecht et al. 2014), the management of IT security risks related to the adoption of cloud services is of significant importance for CIs.

## 1.2 Aim and Structure

Following the outlined importance of IT security risk management for critical infrastructures, the increasing adoption of cloud services by CI providers, and the risks associated with the use of cloud computing solutions, the purpose of this doctoral thesis is to explore the topic of the IT security risk management of cloud computing services in CIs from the perspectives of cloud computing service and CI providers. The overall aim is to contribute to a secure integration and an effective IT security risk management of cloud computing services in critical infrastructures by providing methods, conceptual models, prototypical tools, action recommendations, and practical and theoretical implications. The diversity of cloud computing and CIs and the different perspectives from which the research area is approached require an adequate combination of qualitative and quantitative research in the selection of research methods. Therefore, a mixed-methods approach (Venkatesh et al. 2013) is adopted to answer the following overarching research questions (RQs):

1. What is the status quo of cloud computing service adoption in German critical infrastructures and which research gaps exist?
2. How can IT security risks resulting from the adoption of cloud computing services be managed adequately in critical infrastructures?
3. Which role does trust play in risk management regarding the interaction between cloud computing service providers and critical infrastructures?
4. How can the IT security risk management of cloud services in critical infrastructures be supported with tools?
5. Which risks potentially result from the adoption of cloud computing services?

Due to the extensiveness of the field, not all factors can be taken into account. For example, the risks associated with the adoption of cloud services are manifold and vary between the selected cloud service and deployment models and even between critical industry sectors (Adelmeyer and Teuteberg 2018a). Thus, the implications drawn from the research results provide an overview of the large variability of the research field.

The succeeding sections of Part A are structured as follows. In Section 2, first, the selection of the research contributions included in this dissertation is justified. Second, the research methods applied are outlined. Third, the selected research contributions are classified in a research framework. Following the structure of the framework, the research methods and the key research findings of the selected contributions are presented in Section 3. To prevent redundancies, a detailed summary is avoided. Instead, the focus is placed on the general description of the applied methods and the main results. In Section 4, the research results are synthesized in the form of implications for theory and practice, limitations, and suggestions for future research. Part A of the doctoral thesis ends with a conclusion in Section 5.

# 2 Research Design

## 2.1 Selection of the Research Contributions

The research contributions included in this cumulative dissertation were published in renowned conference proceedings of international scientific conferences or prestigious scientific journals. Each contribution was generally assessed by multiple independent reviewers in a double-blind peer review process. Table 1 provides an overview of the individual research contributions A to K, including their bibliographic information and their respective rankings according to the established ranking system Jourqual 3 (VHB 2015) of the VHB and the orientation list of the WKWI (Heinzl et al. 2008).

| # | Title *(Translation)* | Medium | Ranking | Publication Sources |
|---|---|---|---|---|
| A | Cloud Computing Adoption in Critical Infrastructures – Status Quo and Elements of a Research Agenda | Conference | WKWI: C<br>VHB: D | Adelmeyer, M.; Teuteberg, F.: Cloud Computing Adoption in Critical Infrastructures – Status Quo and Elements of a Research Agenda, in: Proceedings of the Multikonferenz Wirtschaftsinformatik (MKWI 2018), Lüneburg, Germany, pp. 1345–1356 *[1] |
| B | Die Auswirkungen des IT-Sicherheitsgesetzes auf die Interne Revision *(The Impacts of the IT Security Law on Internal Auditing)* | Journal | WKWI: –<br>VHB: D | Goldshteyn, M.; Adelmeyer, M.: Die Auswirkungen des IT-Sicherheitsgesetzes auf die Interne Revision, Zeitschrift Interne Revision (50:6), 2015, pp. 244–255 *[2] |
| C | IT-Risikomanagement von Cloud-Services in Kritischen Infrastrukturen *(IT Risk Management of Cloud Services in Critical Infrastructures)* | Book | WKWI: B *[3]<br>VHB: D *[3] | Adelmeyer, M.; Petrick, C.; Teuteberg, F.: IT-Risikomanagement von Cloud-Services in Kritischen Infrastrukturen, Wiesbaden, Germany: Springer Vieweg, 2018 *[1] *[4] |
| D | Trust Transitivity and Trust Propagation in Cloud Computing Ecosystems | Conference | WKWI: A<br>VHB: B | Adelmeyer, M.; Walterbusch, M.; Biermanski, P.; Teuteberg, F.: Trust Transitivity and Trust Propagation in Cloud Computing Ecosystems, in: Proceedings of the 26th European Conference on Information Systems (ECIS 2018), Portsmouth, UK *[1] *[5] |
| E | Eye-Tracking zur Untersuchung von Vertrauenssignalen auf Webseiten von Cloud Computing-Anbietern *(Eye-Tracking for the Investigation of Trust Signals on Websites of Cloud Computing Providers)* | Conference | WKWI: B<br>VHB: C | Adelmeyer, M.; Beinke, J. H.; Walterbusch, M.; Gameiro, R. R.; König, P.; Teuteberg, F.: Eye-Tracking zur Untersuchung von Vertrauenssignalen auf Webseiten von Cloud Computing-Anbietern, in: Proceedings of the 46. Jahrestagung der Gesellschaft für Informatik (INFORMATIK 2016), Klagenfurt, Austria *[1] *[6] |
| F | Does the Augmentation of Service Level Agreements Affect User Decisions in Cloud Adoption Scenarios? – An Experimental Approach | Conference | WKWI: A<br>VHB: B | Adelmeyer, M.; Walterbusch, M.; Seifert, K.; Teuteberg, F.: Does the Augmentation of Service Level Agreements Affect User Decisions in Cloud Adoption Scenarios? – An Experimental Approach, in: Proceedings of the 24th European Conference on Information Systems (ECIS 2016), Istanbul, Turkey *[1] *[7] |
| G | Datenanalysen in der Cloud – Konzeption einer Architektur für die Wirtschaftsprüfung *(Data Analyses in the Cloud – Conception of an Architecture for Auditing)* | Book Chapter | WKWI: B *[8]<br>VHB: D *[8] | Adelmeyer, M.; Teuteberg, F.: Datenanalysen in der Cloud – Konzeption einer Architektur für die Wirtschaftsprüfung, in Cloud Computing, S. Reinheimer (ed.), Wiesbaden, Germany: Springer Fachmedien, pp. 89-102 *[1] |
| H | RisCC – A Risk Management Tool for Cloud Computing Environments | Conference | WKWI: B<br>VHB: D | Adelmeyer, M.; Beike, L.; Buggenthin, M.; Osada, S.; Teuteberg, F.: RisCC – A Risk Management Tool for Cloud Computing Environments, in: Proceedings of the 24th Americas Conference on Information Systems (AMCIS 2018), New Orleans, LA, USA *[1] *[9] |
| I | Datenschutz und Datensicherheit im Cloud Computing – Ein Framework zur Beurteilung von Cloud-Services *(Data Privacy and Data Security in Cloud Computing – A Framework for the Evaluation of Cloud Services)* | Journal | WKWI: –<br>VHB: C | Adelmeyer, M.; Walterbusch, M.; Lang, J.; Teuteberg, F.: Datenschutz und Datensicherheit im Cloud Computing – Ein Framework zur Beurteilung von Cloud-Services, Die Wirtschaftsprüfung (70:1), pp. 35-42 *[1] *[10] |

| # | Title *(Translation)* | Medium | Ranking | Publication Sources |
|---|---|---|---|---|
| J | Security and Privacy of Personal Health Records in Cloud Computing Environments – An Experimental Exploration of the Impact of Storage Solutions and Data Breaches | Conference | WKWI: A<br>VHB: C | Adelmeyer, M.; Meier, P.; Teuteberg, F.: Security and Privacy of Personal Health Records in Cloud Computing Environments – An Experimental Exploration of the Impact of Storage Solutions and Data Breaches, in: Proceedings of the 14th International Conference on Wirtschaftsinformatik (WI 2019), Siegen, Germany *[1] *[11] |
| K | Rebound Effects in Cloud Computing: Towards a Conceptual Framework | Conference | WKWI: A<br>VHB: C | Adelmeyer, M.; Walterbusch, M.; Biermanski, P.; Seifert, K.; Teuteberg, F.: Rebound Effects in Cloud Computing: Towards a Conceptual Framework, in: Proceedings of the 13th International Conference on Wirtschaftsinformatik (WI 2017), St. Gallen, Switzerland *[1] *[12] |

**Comments**

*[1] Prof. Dr Frank Teuteberg critically reflected on the content and the methodological orientation of each contribution.

*[2] Mr. Michael Goldshteyn is primarily responsible for the section on the principles of the IT Security Law (Section 2) and the text editing.

*[3] The contribution was originally published in the journal “HMD – Praxis der Wirtschaftsinformatik” (VHB: D, MKWI: B) (Adelmeyer, Petrick, et al. 2017). The contribution was honored with the journal's “Best Paper Award 2017” and was selected by the editors for republication as a distinct book, for which the contribution has been considerably revised and extended.

*[4] Mr. Christopher Petrick made a noteworthy contribution to this article, in particular in the operational execution of the expert interviews and the initial interpretation of the acquired data.

*[5] Mr. Peter Biermanski made a noteworthy contribution to this article, in particular in the operational execution of the experiment, the literature search, and the initial interpretation of the acquired data. Dr. Marc Walterbusch supervised the data acquisition and analysis.

*[6] Mr. Jan Heinrich Beinke made a noteworthy contribution to this article, in particular in the operational execution of the eye-tracking study, the literature search, the initial interpretation of the acquired data, and the writing of the article. Dr. Marc Walterbusch supervised the data acquisition and analysis. Mr. Ricardo Ramos Gameiro assisted in the operational execution of the eye-tracking study. Prof. Dr. Peter König critically reflected on the content and methodological orientation of the contribution.

*[7] Mr. Kai Seifert made a noteworthy contribution to this article, in particular in the operational execution of the experiment, the literature search, and the initial interpretation of the acquired data. Dr. Marc Walterbusch supervised the data acquisition and analysis and is responsible for the initial preparation of the contribution, which was considerably revised and presented at the respective conference by the author of this dissertation.

*[8] The contribution was originally published in the journal “HMD – Praxis der Wirtschaftsinformatik” (VHB: D, MKWI: B) (Adelmeyer and Teuteberg 2016). The contribution was selected by the editors for republication in a special edition. In this course, the initial contribution has been considerably revised and extended.

*[9] Mr. Lukas Beike, Mr. Mirko Buggenthin and Mr. Sebastian Osada made noteworthy contributions to this article, in particular in the operational execution of the expert interviews, the literature search, the development, and the initial interpretation of the acquired data.

*[10] Mr. Julian Lang made a noteworthy contribution to this article, in particular in the operational execution of the expert interviews, the literature search, and the initial interpretation of the acquired data. Dr. Marc Walterbusch supervised the data acquisition and analysis.

*[11] Mr. Pascal Meier worked in equal parts on the conception and execution of the experiment as well as on the theoretical foundation of the contribution.

*[12] Mr. Peter Biermanski and Mr. Kai Seifert made noteworthy contributions to this article, in particular in the operational execution of the case study, the literature search, and the initial interpretation of the acquired data. Dr. Marc Walterbusch supervised the data acquisition and analysis and is responsible for the initial preparation of the contribution, which was considerably revised and presented at the respective conference by the author of this dissertation.

**Legend**

VHB = Verband der Hochschullehrer für Betriebswirtschaftslehre (*Translation: German Academic Association for Business Research*) – Journal Quality Index 3 (VHB 2015)

WKWI = Wissenschaftliche Kommission Wirtschaftsinformatik – Orientierungsliste 2008 (*Translation: Scientific Commission Information Systems – Guidance List 2008*) (Heinzl et al. 2008)

Table 1. Overview of the Selected Research Contributions

In addition to the publications presented in Table 1, further articles were published within the context of the research project, which, however, do not fall within the focus of the dissertation and are therefore not included. Contributions C and G, which were originally published in the journal "HMD – Praxis der Wirtschaftsinformatik", occupy a special position, as they were selected for extension and republication by the respective journal editors. Both publications were extensively revised and republished as a book chapter (Contribution G) or an independent book (Contribution C). The initial version of Contribution C was further honored with the journal's Best Paper Award 2017 (Adelmeyer, Petrick, et al. 2017). In total, seven contributions from conferences, two contributions from specialist journals, one book chapter, and one book are included in this cumulative dissertation.

Due to the treatment of German national legal specifics, such as the German IT Security Law and data privacy acts, Contributions B, C, G, and I were prepared in German and placed in corresponding specialist outlets. With the exception of Contribution E, the remaining contributions were written in English. Since the implications and results derived from the contributions have general validity for the IT security risk management of cloud services in critical infrastructures, the dissertation was prepared in English.

## 2.2 Spectrum of Methods

A research methodology can generally be described as “strategy of inquiry used to answer a specific research question” (Recker 2013). In the Information Systems discipline, the research methodology is discussed on two levels (Wilde and Hess 2007). At the aggregated, paradigm-oriented level, a distinction is made between behavioral science and design science (Hevner et al. 2004; Österle et al. 2011). The behavioral science paradigm aims at the development and verification of theories that explain or predict behavior in a human or organizational context, whereas the design science paradigm seeks to build and evaluate new and innovative artifacts (such as models, methods or systems) (Hevner et al. 2004; Peffers et al. 2007; Wilde and Hess 2007). On the methodological level, this aggregated view is broken down into the analysis of individual research methods as systems of procedural rules on which individual research projects are based (Wilde and Hess 2007).

Generally, these methods can be divided into quantitative, qualitative, and mixed-method (Creswell and Creswell 2018), the last of which combining characteristics of quantitative and qualitative research methods in the same inquiry (Myers 2013; Recker 2013; Venkatesh et al. 2013). Considering the specific characteristics, strengths, and weaknesses of the qualitative and quantitative methods, a combination of research methods is often an effective solution for achieving a research objective (Creswell and Creswell 2018; Gable 1994; Jick 1979; Recker 2013). Hence, different perspectives, methods, and data sources were combined within both the individual contributions and the cumulative dissertation as a whole. The present dissertation is therefore to be subordinated to a mixed-methods approach (Venkatesh et al. 2013) in which both qualitative and quantitative aspects and methods are applied (Jick 1979; Myers 2013). Since cloud computing represents an emerging topic and the area of IT security risk management of cloud services in critical infrastructures is not yet well developed (Adelmeyer and Teuteberg 2018a), a focus was put on qualitative research methods, which are particularly suitable for exploratory fieldwork (Myers 2013; Recker 2013). At the paradigm level, elements of both paradigms – behavioral (esp. Contributions D, E, F, and J) and design science research (esp. Contributions G and H) – were incorporated into this dissertation.

Table 2 provides an overview of the research methods applied in the preparation of the respective research contributions listed in Table 1. A detailed discussion of the applied methods can be found in the respective research contributions or references provided in Table 2.

| | Research Method | Contribution | | | | | | | | | | | References |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | A | B | C | D | E | F | G | H | I | J | K | |
| Qualitative | Systematic Literature Review | X | X | X | X | X | X | X | X | X | X | X | vom Brocke et al. (2009), Webster and Watson (2002) |
| | Expert Interviews | X | | X | | | | X | X | X | | X | Gläser and Laudel (2010), Liebold and Trinczek (2009), Meuser and Nagel (2009), Patton (2015), Walsham (2006) |
| | Case Study | | | | | | | | | | | X | Benbasat et al. (1987), Bonoma (1985), Darke et al. (1998), Dubé and Paré (2003), Gable (1994), Kaplan and Duchon (1988), Recker (2013), Yin (2018) |
| | Prototyping | | | | | | | X | X | | | | Davis (1992), Hevner et al. (2004), Hevner (2007) |
| | Other Qualitative Analyses | X | X | X | | X | | X | X | | | | Kaplan and Maxwell (1994), Myers (2013), Patton (2015), Recker (2013), Wilde and Hess (2007) |
| Quantitative | Experiment | | | | X | | X | | | | X | | Aronson and Carlsmith (1968), Recker (2013), Reips (2002), Shadish et al. (2002), Wilde (2008) |
| | Eye-Tracking | | | | | X | | | | | | | Blake (2013), Duchowski (2007), Holmqvist et al. (2011), Kandel et al. (2012) |
| | (Web-based) Survey | | | | | X | | | X | | | | Recker (2013), Reips (2002) |

Table 2. Spectrum of the Applied Research Methods

## 2.3 Framework of the Research Contributions

The research contributions included in this doctoral thesis were each the subject of an independent, fundamental research process that was tailored to the individual research project and research questions. Nevertheless, all research contributions completed the fundamental phases of i) problem identification, formulation, and literature analysis, ii) the development of a research design strategy, iii) data collection and preparation, and iv) the interpretation of the results (Cooper and Schindler 2014; Jenkins 1985). Furthermore, all individual contributions are part of an overall research project and framework that seeks to investigate the IT security risk management of cloud computing services in critical infrastructures. Following the focus of the overarching RQs proposed in Section 1.2, each contribution aims at investigating distinct RQs covering separate subareas of the research field. The research field is divided into three sections (see Figure 1), which determine the structure of the research results section (see Section 3). Due to review procedures, revisions, and resubmissions, the order of the contributions in the framework does not follow the respective chronological publication dates.

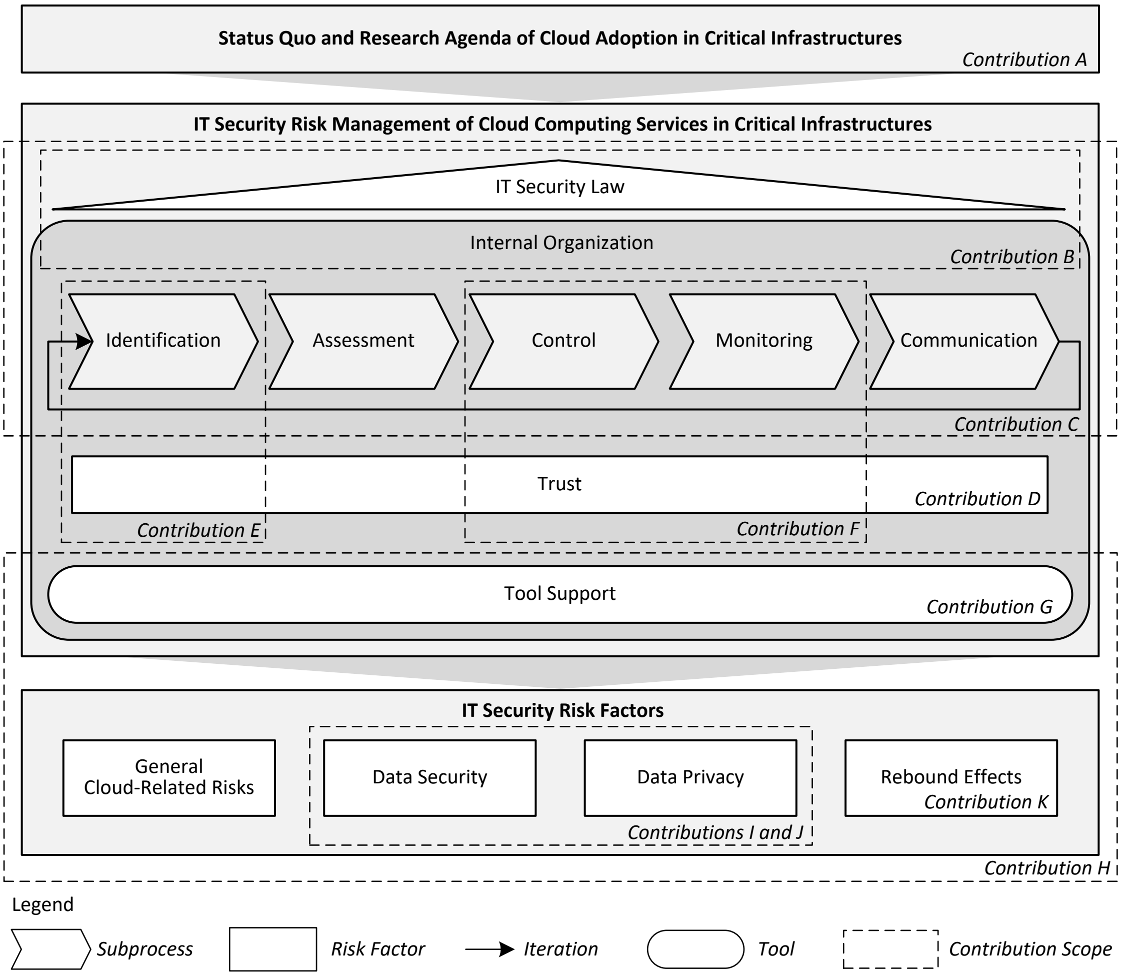

Figure 1. Framework of the Research Contributions

First, in Contribution A, the status quo of cloud computing adoption in CIs is examined (Adelmeyer and Teuteberg 2018a) (see Section 1.2, RQ 1). Additionally, research gaps and issues were identified and synthesized in a research agenda for cloud adoption in CIs. The open research issues identified in Contribution A serve as underlying guidance for the dissertation. However, due to the extensiveness of the field, the proposed agenda is only covered partially in the course of the dissertation, primarily focusing on IT security risk-related research propositions.

Second, the management of IT security risks resulting from the adoption of cloud computing services in CIs is explored (see Section 1.2, RQ 2) based on the findings of Contribution A. In this context, Contribution B investigates the impact of the German IT Security Law on the internal revision of CIs (Goldshteyn and Adelmeyer 2015), as it decisively determines the necessity for an IT security risk management of cloud services in critical infrastructures. In addition to the general implications of the law the affected sectors and the resulting requirements are outlined. Proceeding from the findings of Contribution B, a requirements catalogue for cloud computing services, a framework for the integration of an IT security risk management of cloud services in CIs, and action recommendations for CI and cloud service providers are proposed in Contribution C (Adelmeyer, Petrick, et al. 2018). The framework follows the phases of a prototypical iterative risk management process (see, e.g., Ackermann 2013; Klipper 2015) and builds the core of the framework of the research contributions (see Figure 1). The model risk management process, which consists of the steps of risk identification, assessment, control, monitoring, and communication, is holistically covered in the framework proposed in Contribution C.

Due to the information asymmetry between cloud providers and end-customers prevailing in the cloud market (Walterbusch and Teuteberg 2012), the risks associated with the adoption of certain cloud services are complex and difficult to assess. Generally, the willingness to take risks can be interpreted as trust (Mayer et al. 1995) and is therefore especially necessary where risks are difficult to determine. Although trust is often discussed together with the concept of risk and is an important factor in business decisions, the role and impact of trust in risk management remain unclear (Das and Teng 2004; Earle 2010; Mayer et al. 1995). Since trust is regarded as a key factor in the interaction of CI and cloud providers (Mackay et al. 2012; Paudel et al. 2014; Schöller et al. 2013), its importance to the IT security risk management of cloud services in CIs needs to be considered (see Section 1.2, RQ 3). The general role of trust in the adoption and use of cloud services and the propagation of trust between cloud service users and providers are examined in Contribution D (Adelmeyer, Walterbusch, et al. 2018). In the study, the transfer of trust in cloud mediators to unknown third-party cloud providers is investigated from the perspective of an end-user in the cloud market. To cope with the information asymmetry, customers look for indicators that correlate with the quality of a provider (Benlian and Hess 2011). Therefore, trust signals placed on the websites of cloud providers are examined in Contribution E (Adelmeyer, Beinke, et al. 2016). In the context of the prototypical risk management process underlying the research framework (see Figure 1), the perceived security regarding provider reliability and certifications serves as an indicator for identifying potential risks associated with the use of a certain provider. To bridge the existing information asymmetry gap between cloud customers and providers in the sense of the principal-agency theory (Pavlou et al. 2007) by building trust, outsourcing contracts between the involved parties are of decisive importance (Clemons and Chen 2011), e.g., in the form of service level agreements (SLAs). In this context, Contribution F investigates the effects of the augmentation of SLAs on end-customers' trust (Adelmeyer, Walterbusch, et al. 2016) with respect to the control and monitoring of the risks associated with the selected cloud service.

Since the risks associated with a cloud service vary depending on the selected service and deployment model (Pearson 2013; Zissis and Lekkas 2012), organizations need to be supported by flexible and customizable IT security risk management tools (see Section 1.2, RQ 4). In Contribution G, the use of cloud services for data analyses in the field of auditing is investigated and a prototypical framework is developed (Adelmeyer and Teuteberg 2018b) that can be adapted by CI and cloud providers for risk-related data analyses. To support the entire risk management process, a risk management tool for cloud environments was developed in Contribution H (Adelmeyer, Beike, et al. 2018). The prototype can be adapted and customized by organizations that use or provide cloud services to support the internal risk management of a cloud service in compliance with the organizations' individual risk profiles. In both research contributions, the respective artifacts have been developed iteratively following the design science principle (Hevner et al. 2004; Österle et al. 2011).

Third, the IT security risk factors associated with the adoption of cloud services in critical infrastructures are investigated (see Section 1.2, RQ 5). In Contribution H, the general cloud-related risks are identified as an underlying risk framework for the developed tool (Adelmeyer, Beike, et al. 2018). A framework for assessing the data security and privacy of cloud services is provided in Contribution I (Adelmeyer, Walterbusch, Lang, et al. 2017), covering the IT security protection goals of confidentiality, integrity, and availability. In the context of the exemplary CI sector healthcare, the impacts of storage solutions and data breaches on the perceived security and perceived privacy in cloud computing environments are examined in an experiment from the perspective of end-customers in Contribution J (Adelmeyer et al. 2019). As an example of the variety of potential risk factors associated with the use of cloud services, rebound effects, which describe feedback mechanisms as a result of which savings from efficiency improvements are not or only partially realized, are investigated in Contribution K (Adelmeyer, Walterbusch, Biermanski, et al. 2017a).

# 3 Summary of the Research Contributions

## 3.1 Status Quo and Research Agenda

Although CIs face strict measures and legislation regarding the security, privacy, and resilience of their IT landscapes (Bless et al. 2013; Hecht et al. 2014) and despite the fact that moving IT systems or processes into a cloud exposes CIs to specific risks (Hudic et al. 2014; Rudolph et al. 2014), the adoption of cloud services by CIs is increasing (Diez and Silva 2011; Hecht et al. 2014; Schöller et al. 2013; Wagner et al. 2015). Thus, to contribute to a secure integration and an adequate risk management of cloud computing services in critical infrastructures, the status quo of cloud service adoption in CIs was examined as the foundation for the cumulative dissertation. The objective of Contribution A, titled *"Cloud Computing Adoption in Critical Infrastructures – Status Quo and Elements of a Research Agenda"*, was to examine the following research questions:

(i) *What is the current status quo of cloud adoption in CIs?*

(ii) *Which open research fields exist in the context of cloud adoption in CIs?*

The overall goal was to determine which systems, processes and functions, cloud service and deployment models, and CI sectors are predominant and which general risks arise from cloud adoption in CIs. Furthermore, a research agenda was developed to outline research propositions for science and practice alike, e.g., regarding risk management. The methodical approach was based on a triangulation of data obtained through a systematic literature review, an analysis of the outsourcings of German CI providers to cloud services, and expert interviews. Initially, a systematic literature analysis was conducted following the approach of vom Brocke et al. (2009) and Webster and Watson (2002) to elaborate upon the state of research on cloud adoption in critical infrastructures. In this step, 25 contributions from peer-reviewed journals and conferences with a focus on cloud adoption in CIs were identified. In addition, to determine the current status quo in practice, an analysis of the outsourcings of CIs to cloud services was conducted. For this purpose, 80 German CI providers were examined regarding the adoption of cloud technology. Due to missing information, publicly available business reports and further public information on cloud adoption obtained from the respective corporate websites were considered. The qualitative content analysis (Myers 2013) was focused on the cloud service (IaaS, PaaS, SaaS) and deployment models (public, private, hybrid and community) in use and the respective processes, systems or business functions that are outsourced to or substituted by cloud technologies. Finally, four expert interviews (Gläser and Laudel 2010) were conducted with employees of CI and consulting companies to validate and extend the findings.

For the practical analysis, information on the adoption of cloud services was found for approximately 22.5% of the 80 investigated CI operators. Because only publicly available information was examined, the actual figure is assumed to be higher. Regarding the systems, processes, and functions, CIs primarily outsource 'non-critical' components to cloud services (Diez and Silva 2011), e.g., sales and distribution systems. Since the risks associated with the adoption of cloud services vary depending on the selected deployment or service model, security requirements and threats need to be considered individually (MacDermott et al. 2013, 2015). Although the control over the underlying cloud infrastructure is fully delegated to the service provider in SaaS and public cloud environments (Diez and Silva 2011), both were found to be among the predominant types of cloud services adopted by CIs. Within the CI sectors, the energy sector was found to be at the forefront of cloud adoption, which is congruent with the literature (Dekker 2012; MacDermott et al. 2013; Younis et al. 2013). Of the risks associated with the adoption of cloud services, those associated with security and resilience are of particular importance (Chochliouros et al. 2015; Hecht et al. 2014; MacDermott et al. 2015; Schöller et al. 2013).

The results of the literature analysis were aggregated in a concept matrix and combined with the results of the expert interviews and the practical analysis to determine open research issues and propositions in the field of cloud adoption by CIs (see Table 3). The corresponding research gaps were subdivided into technical (T), jurisdictional (J), organizational (O), and contractual (C) issues. Due to the extensiveness of the field and the research gaps identified in the research agenda, it is not possible to cover all issues in this doctoral thesis. Given the previously outlined dependency of CIs on cloud service providers resulting from a delegation of control, the criticality of the associated security and resilience risks and the importance of the proper IT security risk management of cloud services (Ackermann 2013), selected research gaps with relevance to risk management were approached in the further course of the dissertation. For example, Contributions B and C address compliance with legislation relevant for CIs (J1, J2) and the compliant integration of security incident reporting to authorities (O3). Contributions D, E, and F investigate the trust relationships between cloud service providers and customers (O2). Contribution F deals with the contractual relationships between customers and cloud service providers in terms of SLAs (C1). In Contributions G and H, tools for the support of a flexible and efficient cloud risk management are developed (O1), which can be adapted by CIs. In this context, Contributions I and J address privacy issues related to the use of cloud services (J3). Contribution K proposes a model to identify rebound effects (O4).

| Gap | No., Research Proposition/Issue | References; Expert Interview ID; Practical Analysis |
|---|---|---|
| T | 1. Analysis of interdependency risks of cloud and CI providers | Chochliouros et al. (2015), Dekker (2012), Diez and Silva (2011), Keller (2016); (1-4) |
| | 2. Hybrid cloud frameworks and environments for CIs | Diez and Silva (2011), MacDermott et al. (2013, 2015), Mackay et al. (2012) (2) {P} |
| | 3. Secure data transfer to third parties over external networks | Mackay et al. (2012), Paudel et al. (2014); (1, 2) |
| | 4. Access controls that meet the security requirements of CIs | Hudic et al. (2014), MacDermott et al. (2015), Mackay et al. (2012), Paudel et al. (2014), Schöller et al. (2013), Younis et al. (2013); (4) |
| | 5. Deployment of critical business functions in (public) clouds | Diez and Silva (2011), Mackay et al. (2012), Piggin (2015); (4); {P} |
| J | 1. Analysis of cloud-related requirements of national laws | Adelmeyer, Petrick, et al. (2017), Chochliouros et al. (2015), Dekker (2012), Mackay et al. (2012); (1, 4) |
| | 2. Legally compliant implementation of requirements at the provider | Florian et al. (2013), Schöller et al. (2013); (1, 2) |
| | 3. Analysis of privacy issues particularly relevant to CIs | Chochliouros et al. (2015), Hudic et al. (2014), MacDermott et al. (2015), Schöller et al. (2013), Younis et al. (2013); (1-4) |
| | 4. Open security standards for cloud migration and deployment in CIs | Paudel et al. (2013, 2014), Wagner et al. (2015); (2) |
| | 5. Legal transparency enforcement regarding data location and security | Florian et al. (2013), Schöller et al. (2013), Wagner et al. (2015); (2) |
| O | 1. Development of flexible cloud risk management solutions for CIs | Adelmeyer, Petrick, et al. (2017), Chochliouros et al. (2015), Hecht et al. (2014), Younis et al. (2013) |
| | 2. Investigation of trust relationships between entities | Diez and Silva (2011), Hudic et al. (2014), Mackay et al. (2012), Paudel et al. (2014), Schöller et al. (2013), Younis et al. (2013); (1, 3) |
| | 3. Cloud integration of security incident reporting to authorities | Adelmeyer, Petrick, et al. (2017), Chochliouros et al. (2015), Dekker (2012), Hudic et al. (2014); (2, 4) |
| | 4. CI-relevant risk models for individual sectors and cloud deployments | Chochliouros et al. (2015), Dekker (2012), Hecht et al. (2014), Wagner et al. (2015) |
| C | 1. Investigation of contractual relationships between CIs and cloud service providers, i.e., enhancement of SLAs or smart contract solutions | Florian et al. (2013), Hudic et al. (2014), Mackay et al. (2012), Niekerk and Jacobs (2013), Schöller et al. (2013), Younis et al. (2013); (2, 4) |
| | 2. Continuous assurance of legal security requirements | Hudic et al. (2014), Mackay et al. (2012), Paudel et al. (2014), Schöller et al. (2013), Tauber et al. (2014), Wagner et al. (2015), Younis et al. (2013); (1, 4) |

Table 3. Research Agenda for Cloud Usage in Critical Infrastructures (Adelmeyer and Teuteberg 2018a)

The literature analysis revealed that despite the extensive coverage of cloud computing in theory as well as in praxis, few articles have approached the topic of cloud computing from a CI perspective (Adelmeyer and Teuteberg 2018a). In addition to the findings regarding the adoption of cloud services in critical infrastructures, the analysis showed that the literature lacks an organizational and legal consideration as well as a use of empirical methods. Furthermore, the analysis revealed several open research issues for cloud adoption in CIs. Particularly, suitable risk management models and solutions that allow for the consideration of individual requirements and national legislation for CIs are missing (Adelmeyer and Teuteberg 2018a), which will be further considered in this dissertation.

## 3.2 Risk Management

### 3.2.1 Internal Organization

The research gaps identified in Contribution A stress the necessity for an analysis of the cloud-related requirements of national laws and the legally compliant implementation of requirements at the provider. Thus, Contribution B, titled *"The Impacts of the IT Security Law on Internal Auditing"* (original title: "Die Auswirkungen des IT-Sicherheitsgesetzes auf die Interne Revision"), deals with the legal requirements of the German IT Security Law and their integration into the internal organization of CI providers. Further, the integration of an incident reporting to the respective authorities, as required by the law, is discussed by answering the following research questions:

(i) *Which requirements for CIs result from the IT Security Law?*

(ii) *How can the internal revision of CIs be integrated to comply with the requirements?*

For this purpose, the IT Security Law, which was adopted in July 2015, was analyzed qualitatively to extract its impact on and the requirements for the internal revision of CIs. This includes the scope of the law, affected sectors, resulting IT security requirements, industry-specific security standards, mandatory IT security audits, establishment of a point of contact, reporting obligations, and participation in the elimination of security vulnerabilities. Furthermore, a literature analysis was conducted focusing on German publications with a scope on the implications of the IT Security Law (vom Brocke et al. 2009). Due to the novelty of the law, only 9 publications covering the impact of the IT Security Law on the internal revision were identified. The literature was analyzed for the impact on and short-term requirements for the affected organizations. In this context, action recommendations, standards, and frameworks applicable for the preparation and implementation of IT security audits, which allow for an integration of IT risk management practices (e.g., COSO-ERM or the ISO 27000 family), were presented. In addition, the analysis revealed that an integration of the requirements of the IT Security Law into the internal organization and management is necessary.

Contributions A and B demonstrate that compliance with legislation affecting CI providers and the resulting requirements need to be integrated and observed in internal structures, i.e., a corporate IT security risk management of cloud services (Ackermann 2013). Therefore, Contribution C, titled *"IT Risk Management of Cloud Services in Critical Infrastructures"* (original title: “IT-Risikomanagement von Cloud-Services in Kritischen Infrastrukturen”), examines the requirements for cloud services resulting from the IT Security Law, the resulting consequences for CIs and cloud providers, and the integration of the requirements into IT risk management structures. The corresponding research questions are:

(i) *Which requirements for cloud computing services result from the IT Security Law?*

(ii) *How can the requirements be integrated and considered in IT security risk management structures?*

Partially, the identified requirements of Contribution B provide the foundation of Contribution C. Based on a further qualitative examination of the law, a requirements catalogue for cloud computing services was derived. Furthermore, a framework for the IT security risk management of clouds in CIs was developed and action recommendations for the involved actors were deduced. Initially, a systematic literature review was conducted to explore the topic and to determine a suitable research approach. In addition to the qualitative analysis of the implications of the IT Security Law (Myers 2013), expert interviews with 6 experts from practice with knowledge in the fields of IT security, IT risk management, and cloud computing were conducted and analyzed qualitatively (Meuser and Nagel 2009). The results from both the analysis of the IT Security Law and the expert interviews were aggregated in the requirements catalogue. The catalogue consists of 23 distinct requirements for CI and cloud service providers. Compliance with the technical and organizational requirements of the law is crucial for CIs. This includes the introduction of an information security management system (ISMS), which can be based on the ISO 27000 series. The respective integration of an essential information security risk management is detailed in ISO 27005. On the basis of the findings, a risk management framework for cloud computing services was developed. The central elements of the framework are a prototypical risk management process (see, e.g., Ackermann 2013; Klipper 2015) and a cloud lifecycle phase (Teuteberg 2015), which need to be considered when deploying cloud services. The framework is suitable for the establishment of IT security risk management structures at CI and cloud service providers alike.

The framework (see Figure 2) focuses on corporate IT security risks, which need to be determined depending on the selected cloud service (IaaS, PaaS, and SaaS) and deployment model (private, public, and hybrid cloud). Furthermore, risks individual to sector-specific regulations need to be integrated by the respective CIs (Adelmeyer and Teuteberg 2018a). For this purpose, applicable standards, frameworks, and best practices are listed to provide guidance in establishing appropriate and individual IT security risk management structures. The presented action recommendations can serve as a basis for the concrete implementation of an IT security risk management process for cloud service and CI providers.

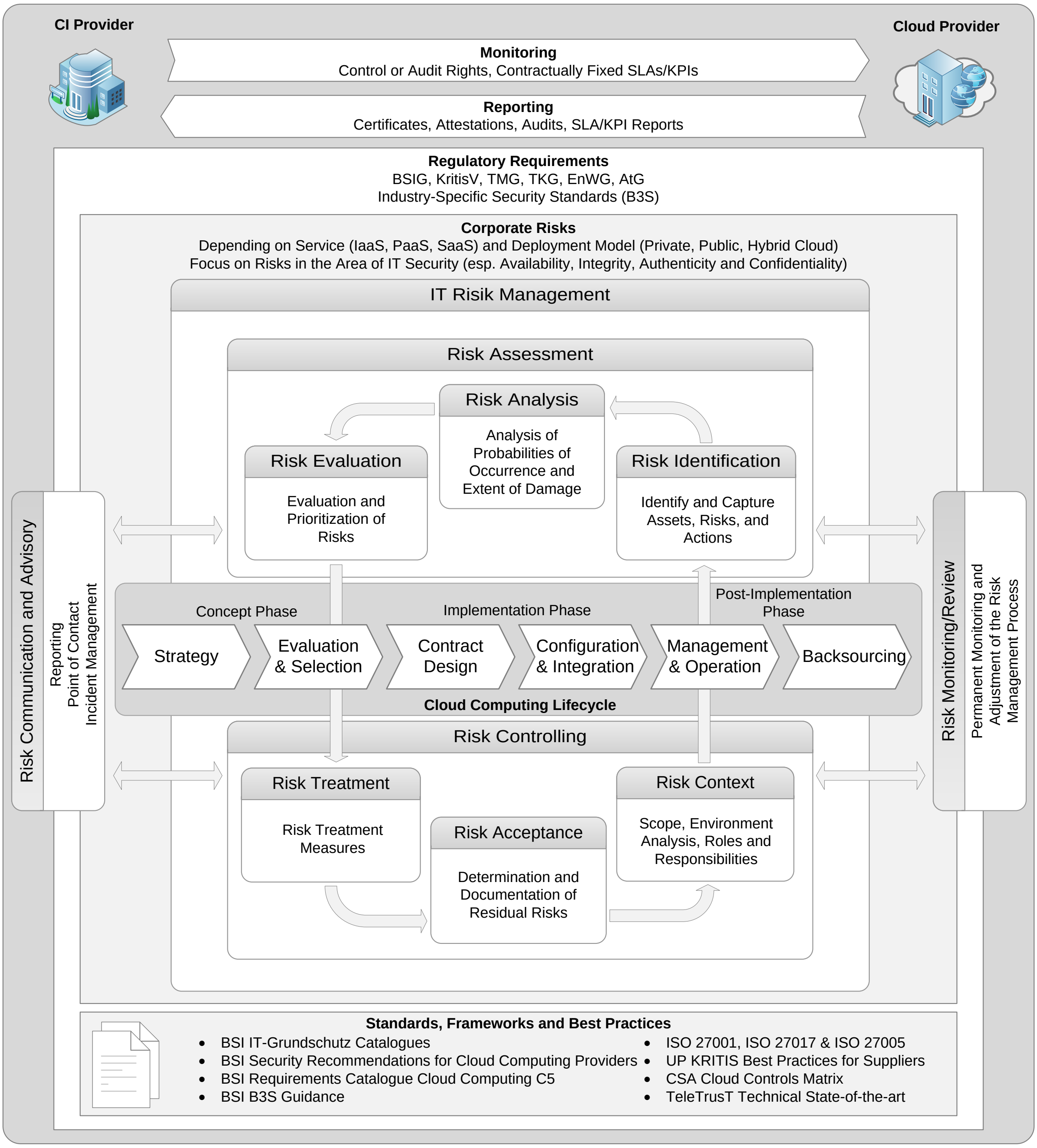
CI Provider
Cloud Provider
Monitoring
Control or Audit Rights, Contractually Fixed SLAs/KPIs
Reporting
Certificates, Attestations, Audits, SLA/KPI Reports
Regulatory Requirements
BSIG, KritisV, TMG, TKG, EnWG, AtG
Industry-Specific Security Standards (B3S)
Corporate Risks
Depending on Service (IaaS, PaaS, SaaS) and Deployment Model (Private, Public, Hybrid Cloud)
Focus on Risks in the Area of IT Security (esp. Availability, Integrity, Authenticity and Confidentiality)
IT Risik Management
Risk Assessment
Risk Analysis
Analysis of Probabilities of Occurrence and Extent of Damage
Risk Evaluation
Evaluation and Prioritization of Risks
Risk Identification
Identify and Capture Assets, Risks, and Actions
Risk Communication and Advisory
Reporting
Point of Contact
Incident Management
Risk Monitoring/Review
Permanent Monitoring and Adjustment of the Risk Management Process
Concept Phase
Implementation Phase
Post-Implementation Phase
Strategy
Evaluation & Selection
Contract Design
Configuration & Integration
Management & Operation
Backsourcing
Cloud Computing Lifecycle
Risk Controlling
Risk Treatment
Risk Treatment Measures
Risk Acceptance
Determination and Documentation of Residual Risks
Risk Context
Scope, Environment Analysis, Roles and Responsibilities
Standards, Frameworks and Best Practices
BSI IT-Grundschutz Catalogues
BSI Security Recommendations for Cloud Computing Providers
BSI Requirements Catalogue Cloud Computing C5
BSI B3S Guidance
ISO 27001, ISO 27017 & ISO 27005
UP KRITIS Best Practices for Suppliers
CSA Cloud Controls Matrix
TeleTrusT Technical State-of-the-art

Figure 2. IT Security Risk Management Framework for Cloud Services in Critical Infrastructures (Adelmeyer, Petrick, et al. 2018)

### 3.2.2 The Role of Trust

Due to the opacity of cloud environments and the information asymmetry between cloud providers and end-customers (Walterbusch and Teuteberg 2012), the risks associated with the adoption of cloud services are complex and difficult to assess. Furthermore, the delegation of control over security measures to the cloud provider and the corresponding dependency on the provider's actions requires trust in the provider on the users' side (Zissis and Lekkas 2012), as not all involved risks can be covered by control mechanisms (Walterbusch et al. 2013). This is especially the case when sensitive systems, data or processes are outsourced to a cloud (Adelmeyer et al. 2019; Adelmeyer, Walterbusch, et al. 2016). Trust can be defined as *"the willingness of a party to be vulnerable to the actions of another party based on the expectation that the other will perform a particular action important to the trustor, irrespective of the ability to monitor or control that other part"* (Mayer et al. 1995). In this context, making oneself vulnerable can be interpreted as a willingness to take risks (Mayer et al. 1995). This is particularly necessary where risks are difficult to determine, as is the case in cloud environments (Adelmeyer, Walterbusch, et al. 2018). Although trust is associated with the concept of risk and constitutes an important factor in business decisions, the role and impact of trust in risk management remains unclear (Das and Teng 2004; Earle 2010; Mayer et al. 1995). Since trust is regarded as a key factor in the interaction of CIs and cloud providers (Mackay et al. 2012; Paudel et al. 2014; Schöller et al. 2013), its role and importance regarding the IT security risk management of cloud services in CIs needs to be investigated.

Therefore, in Contribution D, titled *"Trust Transitivity and Trust Propagation in Cloud Computing Ecosystems"*, the role of trust and its transitivity or propagation between the entities of a trust chain is explored. By applying an experimental vignette study (Aguinis and Bradley 2014; Finch 1987) in a randomized posttest-only design (Recker 2013), Contribution D seeks to answer the following research questions:

(i) *Is trust between a customer, mediator, and service provider in cloud ecosystems transitive?*

(ii) *How do incidents at providers and mediators in cloud ecosystems affect individual end-customers' levels of trust in the respective actors?*

In cloud computing markets, services are often provided indirectly via intermediary parties, who aggregate, integrate, customize or bundle existing third-party basic cloud services and act as so-called cloud mediators on the market (Leimeister et al. 2010). This indirect provisioning of cloud services results in a network of trust relationships between the entities (Lansing and Sunyaev 2016) (see Figure 3).

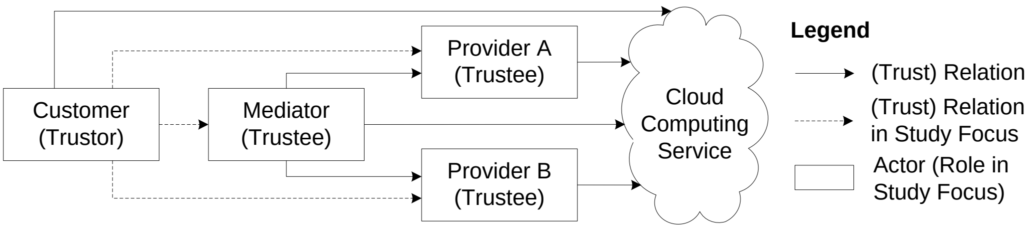

Figure 3. Simplified Trust Chain of Cloud Ecosystem Actors (Adelmeyer, Walterbusch, et al. 2018)

The transfer of a certain level of trust from one entity to another (unknown) entity is referred to as transitivity or propagation, whereby transitivity only occurs in case of complete propagation (Sherchan et al. 2013). In trust propagation, a trustor or customer (Party A, e.g., a CI provider) can derive a certain level of (indirect) trust in an indirectly known cloud provider (Party C) based on its trust in a directly known intermediary party (Party B) (see Figure 4).

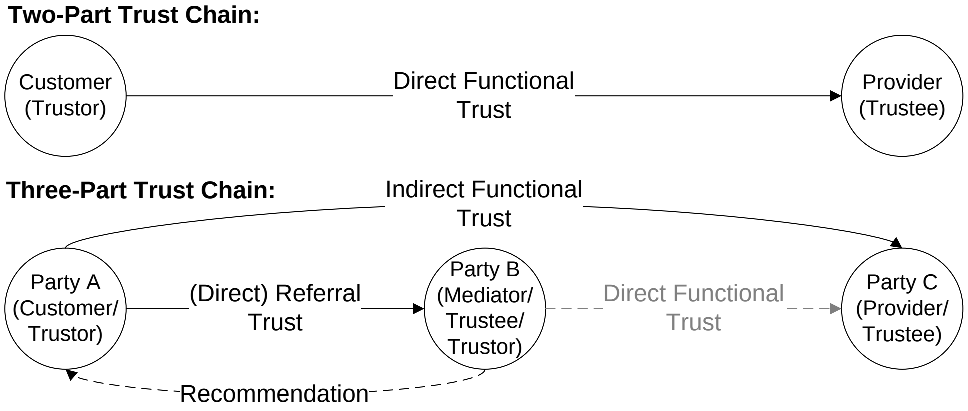

Figure 4. Trust Chains (Adelmeyer, Walterbusch, et al. 2018)

Since the reliability of cloud services is an important factor for CIs (Diez and Silva 2011), Contribution D investigates the impact of a service failure on customers' trust. Based on the theory of reasoned action (Fishbein and Ayzen 1975) and relevant literature from the field of information systems, hypotheses were formulated that reflect the presumed causal relationships between direct functional (DFT), indirect functional (IFT) and referral trust (RT), and the intention to use a provider (ITUP) or a mediator (ITUM). In the vignette, the participants took the roles of customers of a cloud service in a business setting. For the empirical validation of the hypotheses, these were summarized in a structural equation model (SEM). The relevant latent constructs were operationalized using items derived from the literature. The measurement data were collected from undergraduate information systems and economics students using an online survey (sample size n = 277) and analyzed using the partial least squares (PLS) method (Lowry and Gaskin 2014; Ringle et al. 2012, 2015) (see Figure 5).

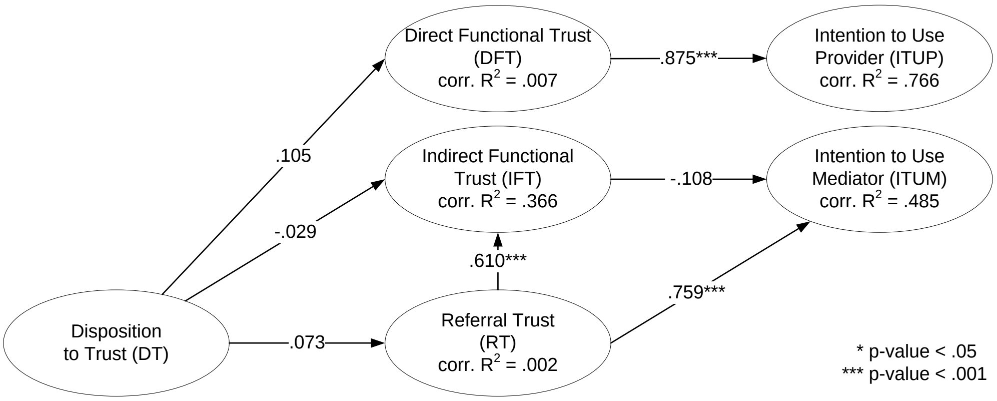
Direct Functional Trust (DFT) corr. $R^2$ = .007
Indirect Functional Trust (IFT) corr. $R^2$ = .366
Referral Trust (RT) corr. $R^2$ = .002
Disposition to Trust (DT)
Intention to Use Provider (ITUP) corr. $R^2$ = .766
Intention to Use Mediator (ITUM) corr. $R^2$ = .485
.105
-.029
.073
.875***
-.108
.610***
.759***
* p-value < .05
*** p-value < .001

Figure 5. PLS Model (Adelmeyer, Walterbusch, et al. 2018)

Regarding the interpretation of the PLS model, path correlations of > .2 indicate significant connections (Chin 1998a) and R²-values of ≈ .33 represent a moderate and R²-values of ≈ .67 a substantial explanation of a construct (Chin 1998b). Following this, the model reveals a significant correlation between the RT in a mediator and the IFT in a provider. Furthermore, by the fact that the IFT is to a moderate extent explained by the RT, the propagation of trust from a mediator to a provider was demonstrated. The study reveals that it is of importance for a customer's trust in a cloud service provider whether a service is obtained directly or indirectly. As cloud services are often provided via mediators, who base their services on adapted basic services of third-party providers (Floerecke and Lehner 2016), the propagation of trust is of crucial significance in cloud computing business relationship chains.

Due to the important role of trust for the selection of reliable cloud service providers and its corresponding significance for adequate risk management measures, Contribution E, titled *"Eye-Tracking for the Investigation of Trust Signals on Websites of Cloud Computing Providers"* (original title: "Eye-Tracking zur Untersuchung von Vertrauenssignalen auf Webseiten von Cloud Computing-Anbietern"), investigates trust signals by cloud providers in an early stage of risk management, i.e., risk identification. As a result of the information asymmetry prevailing in the cloud computing market, customers are looking for quality indicators from providers (Benlian and Hess 2011). Based on the signaling theory (Ross 1977; Spence 1973), trust signals (e.g., certificates or provider reliability) can help to bridge this information asymmetry by "signaling" relevant information. Due to the anonymity of the cloud market, the acquisition of information between customers and cloud service providers often takes place via the providers' website (Adelmeyer, Beinke, et al. 2016). Thus, the following research question was addressed in Contribution E:

*How are trust-influencing factors perceived on cloud service providers' websites?*

To answer the RQ, an eye-tracking study was conducted with 20 student participants. In a single-group posttest-only design, different screenshots of a website of a fictitious cloud provider were presented to the participants for 45 seconds, in which their gaze fixations were recorded and visualized in heat maps (see Figure 6). This enables a qualitative descriptive evaluation and thus observations on which features are perceived more strongly (Blake 2013).

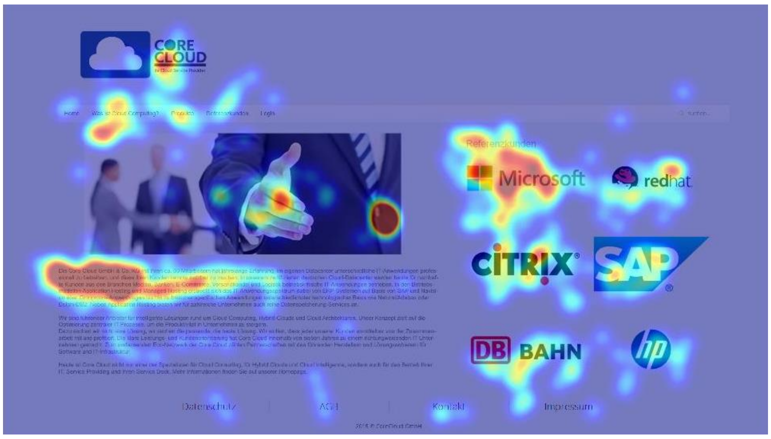

Figure 6. Exemplary Heatmap (Adelmeyer, Beinke, et al. 2016)

Since the meaning of single-gaze tracking or heat maps regarding underlying motives or subjective evaluations is limited, a multi-method design should be applied (Blake 2013; Bojko 2009). In the study, the gaze tracking was combined with a posttest survey to collect data on the participants' assessment of the trust-influencing factors (see Table 4).

| Construct | Trust-Influencing Factor | Sum of Fixations | Survey Mean |
|---|---|---|---|
| Social Presence | *Customer Reviews* | 1247 | 2,825 |
| Perceived Security | *Certifications* | 896 | 3,950 |
| Perceived Security | *Reliability* | 583 | 3,725 |
| Social Presence | *Reference Customers* | 424 | 3,325 |

Table 4. Combined Ranking of Trust-Influencing Factors (Adelmeyer, Beinke, et al. 2016)

In the course of the survey, the respondents were asked to answer various questions about the individually perceived relevance of the trust-influencing factors using a five-point Likert scale ranging from 1 "do not agree" to 5 "do agree". The comparison of the mean values of the assessment from the survey with the sums of the absolute gaze fixations in the corresponding areas of interest provides various possibilities for interpretation, which illustrates the deficits of the evaluation of the absolute number of fixations (Blake 2013). Customer reviews and certificates were most frequently fixated by the subjects. However, the customer reviews were rated less relevant within the survey. Due to the different workloads for conceiving the trust-influencing factors, the subjective evaluation and the corresponding absolute fixations deviate to a certain extent. Nevertheless, it can be concluded that customer reviews are subjectively perceived as less trust-building and further require a higher workload in conception. Certificates and reliability details are perceived as having a similar positive influence on trust and are fixated relatively often. Reference customers are perceived as moderately trust-influencing and are relatively little fixated. In summary, trust-influencing factors placed on providers' websites focusing on the perceived security play an important role in the identification of risks related to the service of a provider, since they were positively assessed and require a relatively low workload for conception and were nevertheless fixated relatively often.

Further important aspects of the IT security risk management of cloud solutions are the monitoring and control of the risks associated with cloud services. In these continuous phases, cloud-related risks are monitored, and the risk management process is controlled and adjusted on the basis of corresponding contractually fixed key figures or so-called service level agreements (Adelmeyer, Petrick, et al. 2018). In the sense of the principal-agency theory (Alchian and Demsetz 1972; Jensen and Meckling 1976), providers need to bridge the existing information asymmetry between customers and providers (Pavlou et al. 2007) by establishing trust and providing comprehensible SLAs. In this context, SLAs, which define the "nature of the underlying service, target performance levels and obligations of the parties involved in the contract", are viewed as an important trust-building factor (Stankov et al. 2012). Following this argumentation, Contribution F, titled *"Does the Augmentation of Service Level Agreements Affect User Decisions in Cloud Adoption Scenarios – An Experimental Approach"*, examines whether the augmentation of specific terms in SLAs affects the (perceived) information overload (IO), the (perceived) comprehension (CO), and the (perceived) transparency (TRA)[1], which affect the ease of use (EOU) and the trusting beliefs (TB), and ultimately the intention to use (ITU) or to adopt a cloud service, by examining the following RQs:

(i) *Does the augmentation of SLAs in the context of cloud computing have an impact on the comprehension of technical terms and parameters?*

(ii) *Does the provision of supplemental information in terms of augmented SLAs in cloud computing have an impact on the trust of (potential) customers in a cloud computing provider?*

Analogous to Contribution D, the research questions were examined in a two-group posttest-only vignette study with 247 undergraduate students. The corresponding hypotheses were de-

[1] In the original research contribution (see Part B), transparency is abbreviated with "TR". To avoid a redundant use of the abbreviation "TR" in this dissertation, transparency is abbreviated with "TRA".

rived from the literature and summarized in an SEM and operationalized as latent constructs in an experimental setup, which was implemented as an online survey. The data was analyzed using the PLS method (Lowry and Gaskin 2014; Ringle et al. 2012, 2015) (see Figure 7).

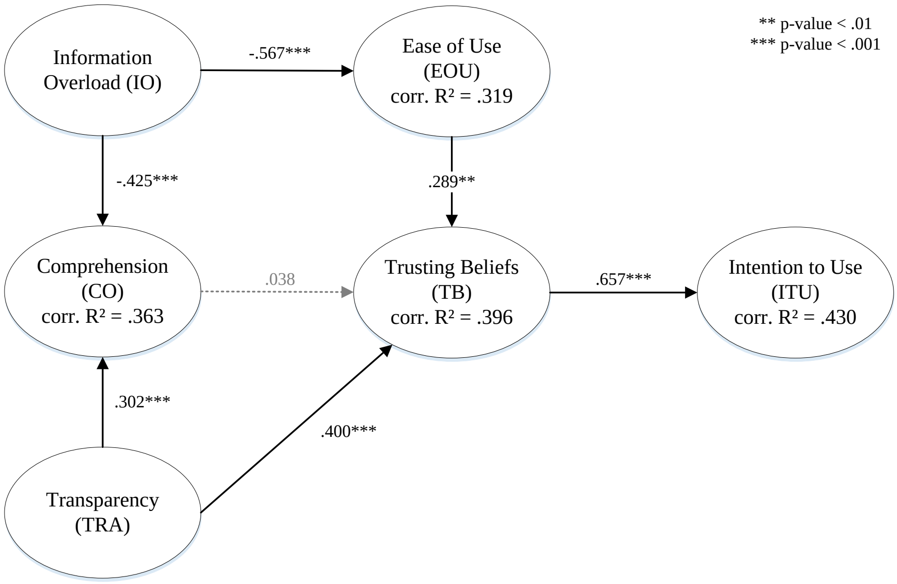
Information Overload (IO)
-.567***
Ease of Use (EOU) corr. R² = .319
** p-value < .01
*** p-value < .001
-.425***
.289**
Comprehension (CO) corr. R² = .363
.038
Trusting Beliefs (TB) corr. R² = .396
.657***
Intention to Use (ITU) corr. R² = .430
.302***
.400***
Transparency (TRA)

Figure 7. PLS Model (Adelmeyer, Walterbusch, et al. 2016)

In the experiment, two groups were defined, of which group 1 was presented an SLA that only consisted of text and group 2 was presented an SLA with augmented key terms, on the basis of which the participants of both groups were asked for their assessment concerning the outlined constructs. In the vignette, the participants were asked to provide a recommendation to their supervisor concerning a fictional cloud computing provider in a business scenario. To validate the hypotheses regarding the effects of the augmentation, an analysis of means (two-sample t-test) was conducted to identify differences between the control group (text only) and the experimental group (augmented SLA). However, the presumed positive effects resulting from an augmentation of SLAs could not be verified (H2, H6, H8) (see Table 1).

| # | Hypotheses | Status |
|---|---|---|
| H1 | A customer's (perceived) trust in a cloud computing provider has a positive effect on the ITU a cloud computing service from this cloud computing provider. | Supported |
| H2 | The provision of augmented SLAs reduces the (perceived) IO. | Not Supported |
| H3 | The (perceived) IO has a negative effect on the (perceived) EOU. | Supported |
| H4 | The (perceived) EOU has a positive effect on the (perceived) TB. | Supported |
| H5 | The (perceived) IO has a negative effect on the (perceived) CO. | Supported |
| H6 | The provision of augmented SLAs increases the (perceived) CO. | Not Supported |
| H7 | The (perceived) CO has a positive effect on the (perceived) TB. | Not Supported |
| H8 | The provision of augmented SLAs increases the (perceived) TRA. | Not Supported |
| H9 | The (perceived) TRA has a positive effect on the (perceived) TB. | Supported |
| H10 | The (perceived) TRA has a positive effect on the (perceived) CO. | Supported |

Table 5. Overview of Hypotheses (Adelmeyer, Walterbusch, et al. 2016)

Nevertheless, the results of the experiment are of potential theoretical and practical value to cloud service providers and their customers. Following the significant impact of TRA on the CO, cloud computing providers need to follow balanced and transparent information policies based on comprehensive, clearly formulated and relevant SLAs. However, information provision might lead to an IO, which again would negatively influence the CO and EOU. Despite the fact that SLAs augmented with background information could not be proven helpful in the study, providers need to evaluate their process and policy of information provisioning to bridge the information asymmetry between customers and providers and ultimately forming trust on the customers' side. Overall, the positive effect of trust coincides with the findings of Contributions D and E and previous studies (cf., e.g., Lansing and Sunyaev 2016; Walterbusch et al. 2013), in which trust was identified as an important requirement and determinant in the context of cloud service provisioning.

### 3.2.3 Tool Support

As a result of the distributed nature of cloud computing and the corresponding control delegation over certain security measures, an efficient risk management needs to be established at both the customer and the provider (Baldwin et al. 2013). However, the majority of existing risk management approaches does not adequately address the monitoring of the security controls and measures associated with cloud computing services (Drissi et al. 2013). This includes the varying risks, which are dependent on the selected service and deployment model and the respective CI sector (Adelmeyer and Teuteberg 2018a; Pearson 2013; Zissis and Lekkas 2012). This fuels the need for flexible risk management tools and solutions that can be tailored individually to cloud adoption or provision scenarios to support the proactive monitoring of cloud-related risks (Djemame et al. 2011; Hecht et al. 2014).

Therefore, in Contribution G, titled *"Data Analyses in the Cloud – Conception of an Architecture for Auditing"* (original title: "Datenanalysen in der Cloud – Konzeption einer Architektur für die Wirtschaftsprüfung"), a prototypical framework for data analysis in cloud environments is developed. Although the focus of the development was put on auditing, the framework can be adapted and implemented for data analyses over the whole IT security risk management process in, e.g., an organization's internal revision (Goldshteyn and Adelmeyer 2015), to cope with the ever-growing amount of data that needs to be analyzed. The corresponding research question is as follows:

*How can extensive data analyses in auditing be supported by cloud computing?*

In addition to a literature analysis of relevant publications in the field of cloud data analyses, a total of 16 guideline-based open expert interviews were conducted at a Big Four auditing company (Meuser and Nagel 2009). In the qualitative analyses, the interview transcripts were coded and categorized. This way, the potential advantages and challenges of such a solution, e.g., data privacy and security aspects, were identified. Following the constructivist paradigm (Wilde and Hess 2007), the findings of the literature analysis and the expert interviews were synthesized to develop a prototypical cloud data analysis framework (see Figure 8).

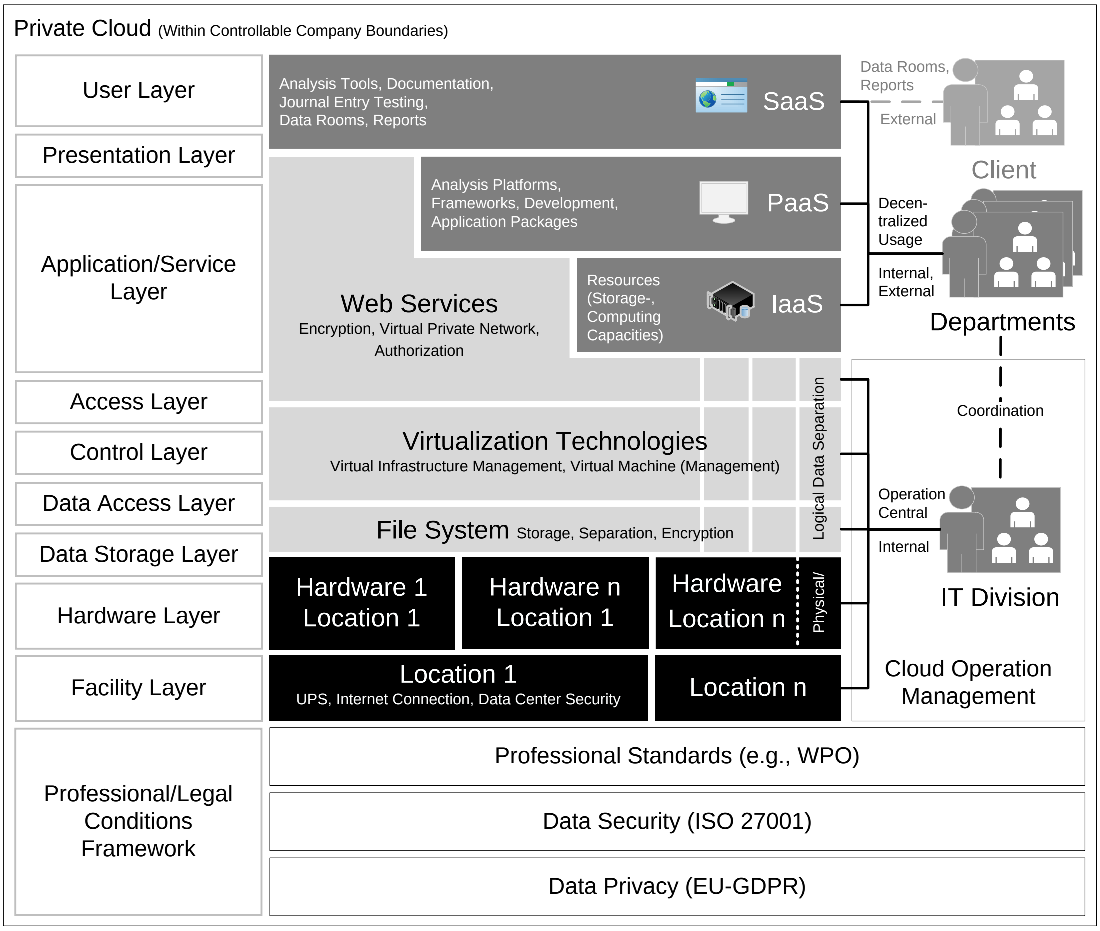
Private Cloud (Within Controllable Company Boundaries)
User Layer
Presentation Layer
Application/Service Layer
Access Layer
Control Layer
Data Access Layer
Data Storage Layer
Hardware Layer
Facility Layer
Professional/Legal Conditions Framework
Analysis Tools, Documentation, Journal Entry Testing, Data Rooms, Reports
SaaS
Analysis Platforms, Frameworks, Development, Application Packages
PaaS
Resources (Storage-, Computing Capacities)
IaaS
Web Services
Encryption, Virtual Private Network, Authorization
Virtualization Technologies
Virtual Infrastructure Management, Virtual Machine (Management)
File System Storage, Separation, Encryption
Logical Data Separation
Hardware 1 Location 1
Hardware n Location 1
Hardware Location n
Physical/
Location 1
UPS, Internet Connection, Data Center Security
Location n
Professional Standards (e.g., WPO)
Data Security (ISO 27001)
Data Privacy (EU-GDPR)
Data Rooms, Reports
External
Client
Decen-tralized Usage
Internal, External
Departments
Coordination
Operation Central
Internal
IT Division
Cloud Operation Management

Figure 8. Data Analysis Cloud Framework (Adelmeyer and Teuteberg 2018b)

Due to the sensitivity of the data, especially in the field of auditing, the framework is based on a private cloud to maintain data sovereignty. Further, the integration of the ISO 27001 certification, which is particularly relevant for CIs (Adelmeyer, Petrick, et al. 2018), needs to be ensured. Although the presented data analysis framework can possibly support the risk management of cloud services in CIs in all phases, it is most valuable for the phases of risk assessment, control, and monitoring, due to its focus on auditing and revision. In summary, the use of cloud computing services for data analyses in auditing has the potential to make data analyses in auditing more efficient and pave the way for new auditing opportunities.

To ensure adequate tool support in all phases of IT security risk management and for individual cloud adoption scenarios, a risk management tool prototype was developed in Contribution H, titled *"RisCC – A Risk Management Tool for Cloud Computing Environments"*. The study follows the research questions of:

(i) *Which cloud-specific risks exist?*

(ii) *How can risk management for cloud services for both cloud service users and providers be efficiently supported by a software solution?*

For the development of the tool, the design science paradigm was adopted to incorporate scientific knowledge and knowledge from the field (Hevner et al. 2004; Österle et al. 2011). In the design science approach, the "Generate/Test Cycle" was applied using several research methods in an iterative process, in which a design is continuously adjusted after constant evaluation. The methods applied include a literature review (vom Brocke et al. 2009), seven expert interviews (Meuser and Nagel 2009) focusing on risk management of cloud solutions, qualitative and quantitative analyses (Myers 2013; Oates 2006), and a survey (Oates 2006). In the literature analysis, 87 relevant articles were identified, of which 13 were found in high-ranked journals, 66 in an open search and eight in a forward and backward search.

In the first step, the requirements for the tool were collected in several iterations. This includes requirements derived from the literature, expert interviews, and qualitative analyses of relevant standards, frameworks and guidelines, and existing cloud risk management software. To incorporate the variety of cloud adoption scenarios and their corresponding risk profiles, the tool and the underlying database model were designed modularly (see Figure 9).

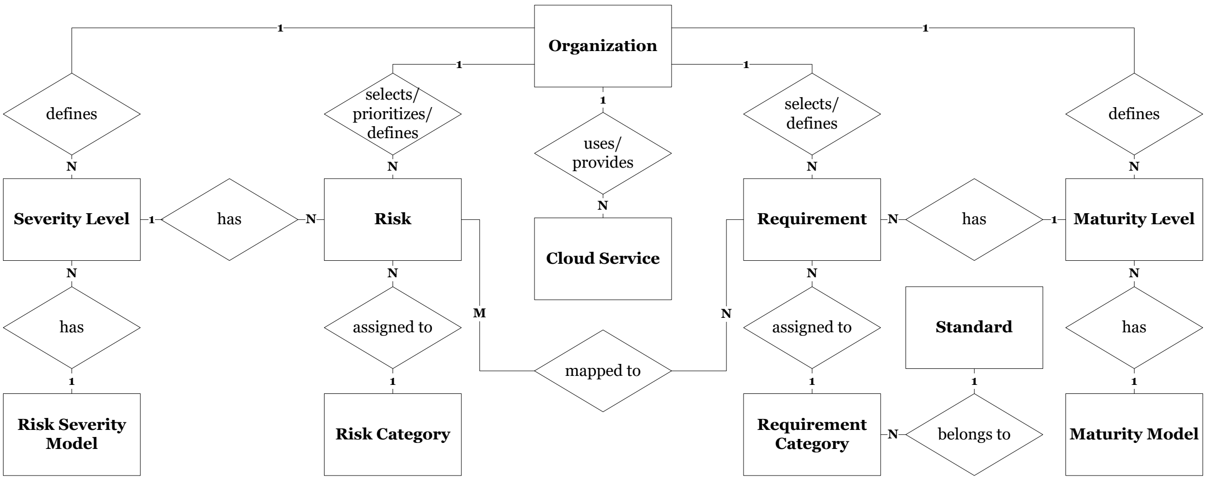

Figure 9. Simplified Database Entity Relationship Model (Adelmeyer, Beike, et al. 2018)

The modular design includes the individual selection of risks, requirements, and maturity and severity levels. Furthermore, existing standards can be fully implemented and adjusted according to the respective cloud adoption scenario. To achieve this, flags in the database tables *Risk* and *Requirement* indicate manual entries. The database model further supports the parallel monitoring of multiple standards or frameworks. The collected requirements were summarized in use cases to detail the initial concept of the solution. Subsequently, the requirements and use cases were implemented as a web-based tool, which was developed on the foundation of a content management system (see Figure 10).

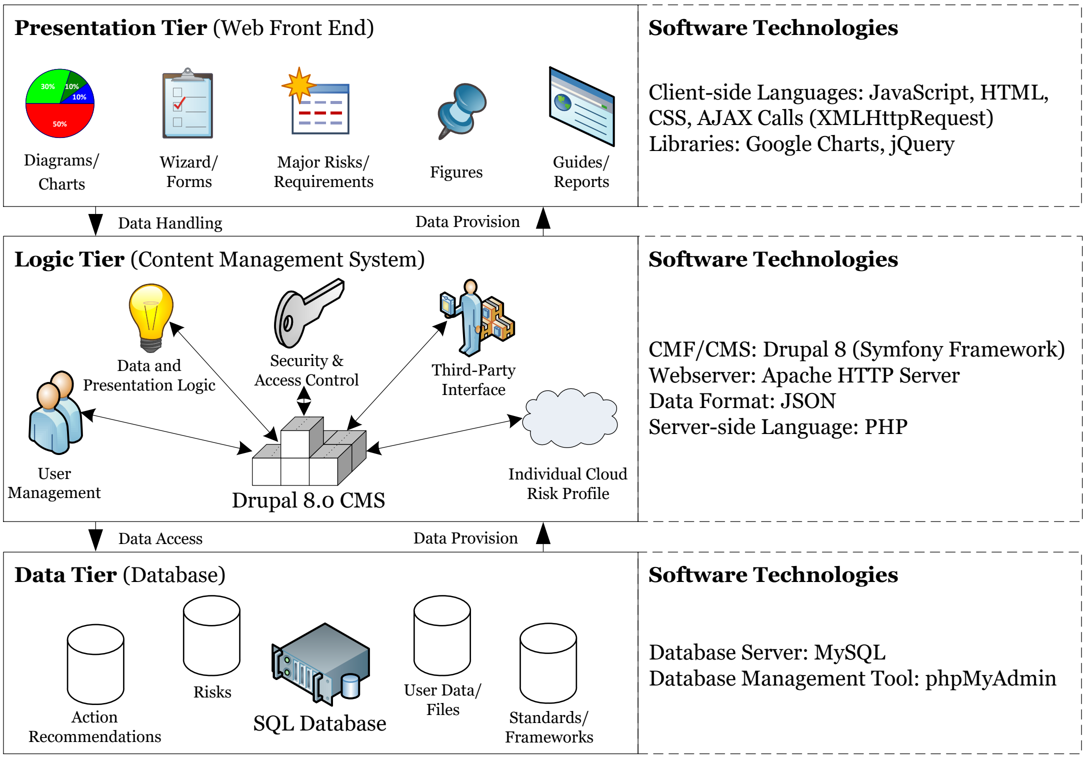
**Presentation Tier** (Web Front End)
30%
10%
10%
50%
Diagrams/ Charts
Wizard/ Forms
Major Risks/ Requirements
Figures
Guides/ Reports
**Software Technologies**
Client-side Languages: JavaScript, HTML, CSS, AJAX Calls (XMLHttpRequest)
Libraries: Google Charts, jQuery
Data Handling
Data Provision
**Logic Tier** (Content Management System)
Data and Presentation Logic
Security & Access Control
Third-Party Interface
User Management
Drupal 8.0 CMS
Individual Cloud Risk Profile
**Software Technologies**
CMF/CMS: Drupal 8 (Symfony Framework)
Webserver: Apache HTTP Server
Data Format: JSON
Server-side Language: PHP
Data Access
Data Provision
**Data Tier** (Database)
Action Recommendations
Risks
SQL Database
User Data/ Files
Standards/ Frameworks
**Software Technologies**
Database Server: MySQL
Database Management Tool: phpMyAdmin

Figure 10. Technical Concept of RisCC (Adelmeyer, Beike, et al. 2018)

The evaluation of the prototype was conducted by surveying five of the seven previously consulted experts. In an online survey, qualitative and quantitative data were collected. Based on an analysis of the data, improvement suggestions were derived that served as the basis for the adjustment of the prototype. Overall, the evaluation proved the usefulness of the developed tool for supporting the risk management of cloud computing services for both cloud service users and providers. With the developed tool, regulatory amendments and industry-specific regulations can be incorporated when monitoring IT security risks resulting from the adoption of cloud services (Adelmeyer, Petrick, et al. 2018; Baldwin et al. 2013). Furthermore, the corresponding risk profiles of individual cloud adoption scenarios can be adequately managed (Adelmeyer and Teuteberg 2018a; Pearson 2013; Zissis and Lekkas 2012).

## 3.3 IT Security Risk Factors

### 3.3.1 Cloud-Related Risk Factors

As previously stated, the risks resulting from specific cloud adoption scenarios vary with the selected cloud service and deployment model and the targeted data and processes, which is why they have to be assessed individually for each cloud adoption scenario (Adelmeyer, Petrick, et al. 2018). Although IT security risks are regarded as the most salient risks related to cloud service adoptions (Ackermann 2013), the resulting risks and threats are manifold (Zissis and Lekkas 2012). To identify the general risk factors that are associated with the adoption of cloud services, the results from the literature analysis and the expert interviews of Contribution H were combined and structured in a concept matrix. The matrix is divided into four risk categories, i.e., *Technical*, *Organizational*, *Legal*, and *Others*, which are derived from Catteddu & Hogben (2009) and Djemame et al. (2011). In the 87 articles examined, a total of 30 risks were identified and assigned to the categories. From the expert interviews, the additional risks "Shadow IT" and "Organization Readiness" were derived (see Table 6).

| **Category** | **Risk (No. of Mentions: Literature Analysis; Expert Interviews)** | |
|---|---|---|
| Technical | • Data Breaches (53; 3)<br>• Service Availability (52; 7)<br>• Malicious Insider (45; 0)<br>• Network Security (44; 2)<br>• Data Encryption (43; 1)<br>• Data Integrity (42; 1)<br>• Infrastructure (37; 0) | • Data Segregation (36; 1)<br>• Resource Exhaustion (35; 2)<br>• Hypervisor Isolation Vulnerabilities (34; 1)<br>• Interface/Service Engine Compromise (32; 1)<br>• Data Deletion/Disposal (23; 3)<br>• Malware (9; 1) |
| Organi-zational | • Privileged User Access and Social Engineering (52; 3)<br>• Long-Term Viability (45; 4)<br>• Vendor Lock-In (44; 3)<br>• Recovery (43; 5) | • Loss of Governance (29; 2)<br>• Loss of Business Reputation (9; 1)<br>• Organization Readiness (0; 3)<br>• Shadow IT (0; 1) |
| Legal | • Regulatory Compliance (55; 4)<br>• Service Level Agreements (45; 5)<br>• Data Location (42; 6)<br>• Data Privacy (40; 1) | • Changes of Jurisdiction (28; 3)<br>• Data Protection Risks (19; 6)<br>• Data Ownership (14; 0) |
| Others | • Natural Disasters (17; 2)<br>• Abuse of Cloud Services (15; 0) | • Economic Risks (12; 3)<br>• Unknown Risks (8; 0) |

Table 6. Identified Risks in Cloud Computing (Adelmeyer, Beike, et al. 2018)

To assure a comparable aggregation level, several identified individual risks were summarized. Table 6 illustrates the extensive number of cloud-related risks that may arise and that need to be considered when adopting a cloud solution within an organization. The concept matrix serves as a basic risk framework for the cloud risk management tool developed in Contribution H. However, the listing does not claim to be exhaustive, since cloud-related risks may arise individually and are dependent on the cloud service and deployment model (Adelmeyer and Teuteberg 2018a; Pearson 2013; Weintraub and Cohen 2016; Zissis and Lekkas 2012).

### 3.3.2 Security and Privacy

In addition to strict regulations regarding the IT security of their systems, CIs need to cope with uncertainties regarding data privacy (Adelmeyer and Teuteberg 2018a). The two concepts of security and privacy are strongly interconnected. Security can be regarded as an overarching principle concerning the general confidentiality, integrity, and availability, whereas privacy focuses on personal or private information (Eckert 2018). Audits and associated certifications can assure compliance with basic and defined standards. However, the requirements for cloud services are specific and the market for existing standards and certificates for cloud services is heterogeneous (Adelmeyer, Walterbusch, Lang, et al. 2017). Thus, Contribution I, titled *"Data Privacy and Data Security in Cloud Computing – A Framework for the Evaluation of Cloud Services"* (original title: "Datenschutz und Datensicherheit im Cloud Computing – Ein Framework zur Beurteilung von Cloud-Services"), addresses the RQ of:

*How can data privacy and data security of cloud computing services be evaluated?*

Initially, a systematic review of the relevant literature was conducted to become more familiar with the complex topic of data privacy and data security in cloud environments to determine a suitable research approach. The article first discusses how to deal with risks arising from the use of cloud services against the background of the generally accepted auditing principles. Afterwards, the role of data privacy and data security audits as well as selected cloud-specific initiatives, standards, guidelines, and certifications are addressed. For the evaluation of data privacy and data security of cloud computing services, a framework is presented, which was developed on the basis of two expert interviews (Meuser and Nagel 2009) with interview partners having many years of experience in the field of data privacy audits. The aim of the framework is to clarify the potential order in which an evaluation of data privacy and data security of cloud computing services is possible and which criteria are to be observed. For this purpose, the complex topic of data privacy and data security in cloud computing is divided into the sub-models Legal Compliance Model, Privacy and Security Compliance Model, and Privacy and Security Control Model (see Figure 11).

In the Legal Compliance Model, the legal and regulatory requirements that cloud computing service providers and customers have to follow when outsourcing functions or processes are determined. The model primarily focuses on legislation in Germany, the EU, and the US. Depending on the underlying service or deployment model, compliance with the relevant statements must be assessed individually. The framework is applicable to the general evaluation of cloud services but allows for the consideration of special requirements for CIs. This includes the integration of industry specifics, standards, and requirements, such as ISO 27000. As the basis for data privacy criteria, the data security requirements derived from the relevant regulations are considered in the Privacy and Security Compliance Model. In the Privacy and Security Control Model, controls and frameworks are presented, by the implementation of which cloud computing providers can meet the most important criteria.

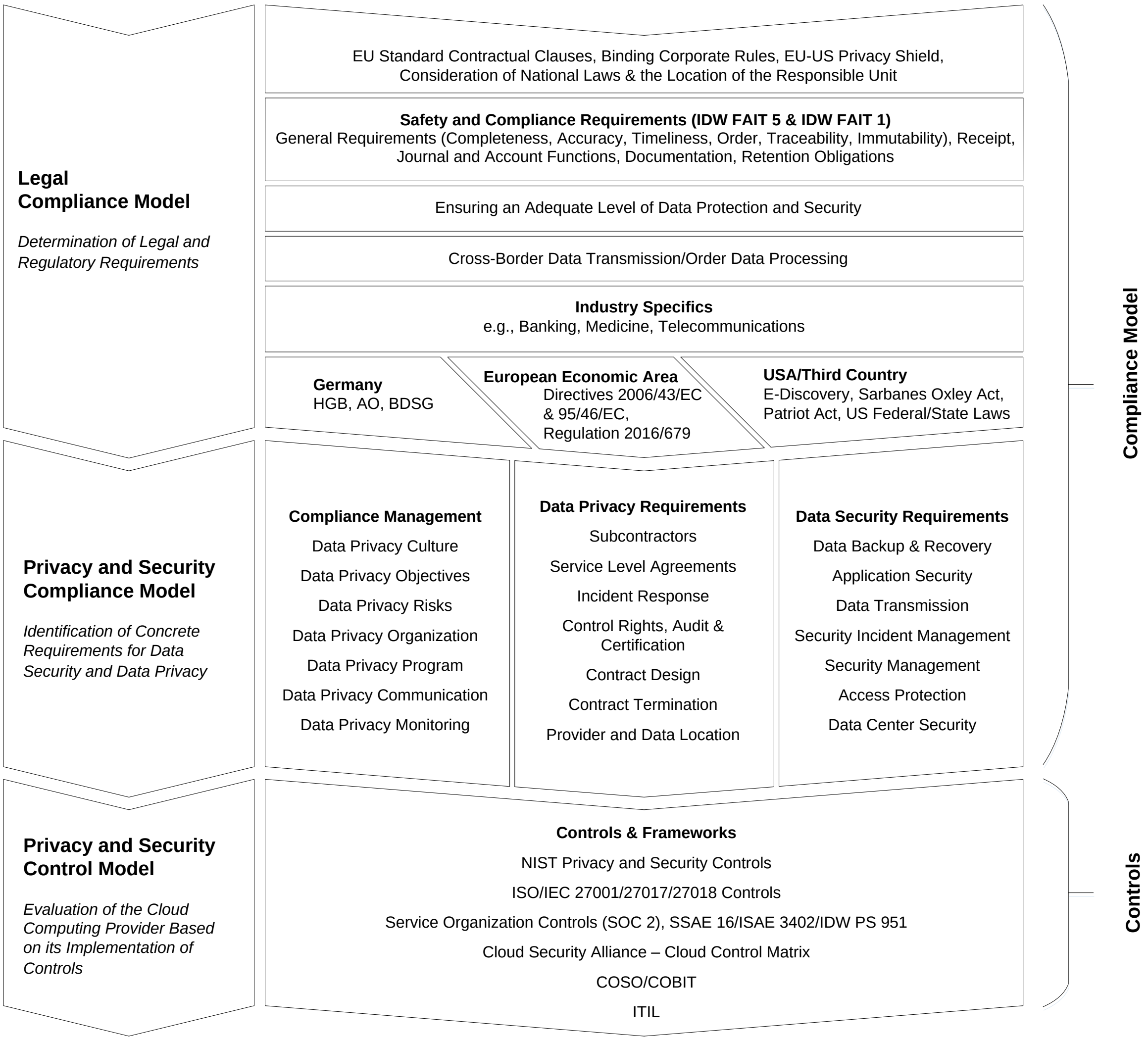
Legal
Compliance Model
Determination of Legal and Regulatory Requirements
EU Standard Contractual Clauses, Binding Corporate Rules, EU-US Privacy Shield, Consideration of National Laws & the Location of the Responsible Unit
Safety and Compliance Requirements (IDW FAIT 5 & IDW FAIT 1)
General Requirements (Completeness, Accuracy, Timeliness, Order, Traceability, Immutability), Receipt, Journal and Account Functions, Documentation, Retention Obligations
Ensuring an Adequate Level of Data Protection and Security
Cross-Border Data Transmission/Order Data Processing
Industry Specifics
e.g., Banking, Medicine, Telecommunications
Germany
HGB, AO, BDSG
European Economic Area
Directives 2006/43/EC & 95/46/EC, Regulation 2016/679
USA/Third Country
E-Discovery, Sarbanes Oxley Act, Patriot Act, US Federal/State Laws
Compliance Model
Privacy and Security
Compliance Model
Identification of Concrete Requirements for Data Security and Data Privacy
Compliance Management
Data Privacy Culture
Data Privacy Objectives
Data Privacy Risks
Data Privacy Organization
Data Privacy Program
Data Privacy Communication
Data Privacy Monitoring
Data Privacy Requirements
Subcontractors
Service Level Agreements
Incident Response
Control Rights, Audit & Certification
Contract Design
Contract Termination
Provider and Data Location
Data Security Requirements
Data Backup & Recovery
Application Security
Data Transmission
Security Incident Management
Security Management
Access Protection
Data Center Security
Privacy and Security
Control Model
Evaluation of the Cloud Computing Provider Based on its Implementation of Controls
Controls & Frameworks
NIST Privacy and Security Controls
ISO/IEC 27001/27017/27018 Controls
Service Organization Controls (SOC 2), SSAE 16/ISAE 3402/IDW PS 951
Cloud Security Alliance – Cloud Control Matrix
COSO/COBIT
ITIL
Controls

Figure 11. Framework for the Evaluation of Privacy and Security of Cloud Services (Adelmeyer, Walterbusch, Lang, et al. 2017)

Due to the large number of requirements, a holistic consideration of all regulations, criteria, and controls in the model is not practical. Rather, the framework has to be evaluated and adapted individually on an industry-specific base. Against the background of heterogeneous audits and certificates, the presented framework provides an approach to assess the most important aspects of data privacy and data security of cloud services. However, the individual conditions of an outsourcing to a cloud (location of the provider, type of data and processes outsourced, etc.) must be taken into account when applying the framework.

Generally, the adoption of cloud computing environments entails risks and challenges for data privacy and data security, especially for CIs (Hudic et al. 2014). Thus, Contribution J, titled *"Security and Privacy of Personal Health Records in Cloud Computing Environments – An Experimental Exploration of the Impact of Storage Solutions and Data Breaches"*, investigates their role in the exemplary CI sector of healthcare for the provisioning of Personal Health Records (PHRs). The contribution seeks to address the following research questions:

(i) *Do patients' perceived security, perceived privacy, trust, and perceived control differ between cloud environments and private on-premise data centers when storing personal health data in PHRs?*

(ii) *In case of a data breach, to which extent do patients' perceived security, perceived privacy, trust, and perceived control differ when using cloud environments compared to private on-premise data centers?*

For this purpose, an experimental study was conducted with 238 student participants who were divided into two experiment groups. In group 1, the personal health data of the participants was outsourced to a public cloud environment, whereas in group 2, a private on-premise data center was used. Both groups were displayed a vignette in which the participants were asked to act as longtime users of a personal health record web-service that centrally stores and manages the users' relevant personal health data. After the initial vignette, a first posttest was conducted, in which the participants' attitudes towards the different storage solutions prior to a data breach were measured. To allow for a comparison of the users' trust (TR), perceived control (CTRL)[2], perceived privacy (PRI), perceived security (SEC), and intention to use (ITU) before and after a data breach, a second posttest was conducted in both groups.

For the testing of the previously formulated hypotheses, the data were analyzed by conducting analyses of means (two-sample t-test) and PLS SEM. To evaluate the differences between the cloud service (G1) and on-premise data center storage (G2) before and after a data breach, the results of the first and the second posttest were compared between both groups. The relationships between the constructs and their impact on the dependent variables were evaluated in a PLS SEM (see Figure 12).

[2] In the original research contribution (see Part B), perceived control is abbreviated with "CO". To avoid a redundant use of the abbreviation "CO" in this dissertation, perceived control is abbreviated with "CTRL".

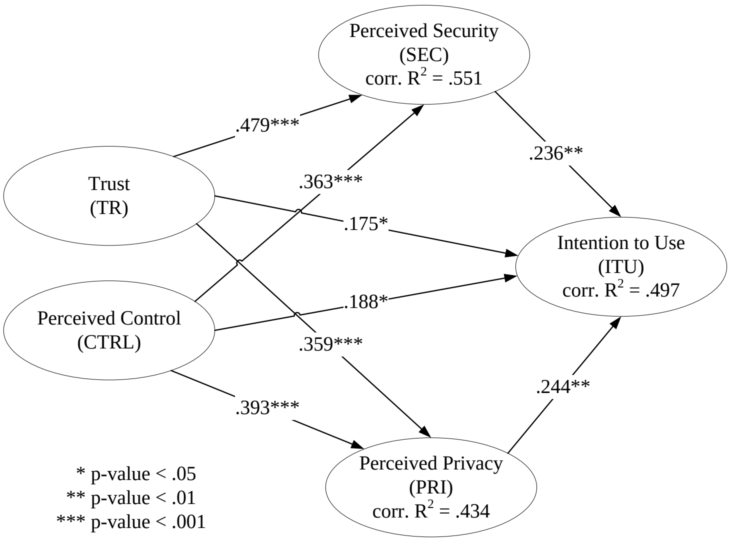

Figure 12. PLS Model (Adelmeyer et al. 2019)

In the model, strong statistically significant relationships between TR and SEC and PRI as well as between CTRL and SEC and PRI can be found. In addition, path coefficients of ≥ .236 between SEC and PRI and the ITU indicate a moderate influence of both constructs on the ITU. Further, since CTRL and TR largely determine SEC and PRI ($R^2$ = .551 and .434), which again have a strong effect on the ITU, a low but significant impact of TR and CTRL on the ITU can be assumed. Regarding the evaluation of the different outcomes of the storage solutions and the data breach, significant differences between G1 and G2 ($p < .05$) could be identified for all constructs. However, after a data breach, no significant differences between the groups (marked with an "E") can be identified for SEC, PRI, and TR with the exception of CTRL. The statuses of the hypotheses are shown in Table 7.

| H | Relation | Status |
|---|---|---|
| 1a | SEC(G2) > SEC(G1) | Supported |
| 1b | SEC(G2E) = SEC(G1E) | Supported |
| 2a | PRI(G2) > PRI(G1) | Supported |
| 2b | PRI(G2E) = PRI(G1E) | Supported |
| 3a | TR(G2) > TR(G1) | Supported |
| 3b | TR(G2E) = TR(G1E) | Supported |
| 4 | TR ↑ ⇒ SEC ↑ | Supported |
| 5 | TR ↑ ⇒ PRI ↑ | Supported |
| 6a | CTRL(G2) > CTRL(G1) | Supported |
| 6b | CTRL(G2E) = CTRL(G1E) | Not Supported |
| 7 | CTRL ↑ ⇒ SEC ↑ | Supported |
| 8 | CTRL ↑ ⇒ PRI ↑ | Supported |
| 9 | SEC ↑ ⇒ ITU ↑ | Supported |
| 10 | TR ↑ ⇒ ITU ↑ | Supported |
| 11 | CTRL ↑ ⇒ ITU ↑ | Supported |
| 12 | PRI ↑ ⇒ ITU ↑ | Supported |

Table 7. Statuses of the Hypotheses (Adelmeyer et al. 2019)

The experiment reveals that the participants' SEC, PRI, CTRL, and TR are significantly higher when personal data in the form of PHRs are stored in on-premise data centers compared to cloud environments. However, this is no longer the case after a data breach, except for CTRL (H6b). Hence, PHR providers need to carefully decide whether to offer their services via (public) clouds or private on-premise environments to minimize concerns on the users' side.

### 3.3.3 Rebound Effects

Although the use of cloud computing services is deemed to be economically beneficial for CIs (Adelmeyer and Teuteberg 2018a), they face economic risks when adopting cloud solutions (Adelmeyer, Beike, et al. 2018). Among the multitude of possible economic risks is the rebound effect, which can basically be described as a feedback mechanism, as a result of which the savings arising from efficiency improvements are not or only partially realized (Gossart 2014). Rebound effects can potentially affect multiple organizational resources, which ultimately affect an organization’s funds (Adelmeyer, Walterbusch, Biermanski, et al. 2017b).

To explore the rebound effects potentially resulting from cloud service adoptions, Contribution K, titled *“Rebound Effects in Cloud Computing: Towards a Conceptual Framework”*, seeks to answer the following research questions:

(i) *How can rebound effects in cloud computing be conceptualized?*

(ii) *Which organizational resources are potentially affected by rebound effects in cloudsourcing scenarios?*

For the initial investigation, a systematic literature review (vom Brocke et al. 2009) focusing on the definition of rebound effects was conducted. Furthermore, the rebound effect phenomenon in cloud computing was explored by means of a synthesized case study approach (Dubé and Paré 2003; Gable 1994; Newell and Simon 1972; Recker 2013), in which an organization was accompanied during a typical cloud adoption and outsourcing process. During the project steps, several data collection methods and sources were used (Benbasat et al. 1987): (i) documentation (e.g., infrastructure plans), (ii) archival records (e.g., organization charts), (iii) interviews (e.g., with the IT decision makers), and (iv) physical artifacts (e.g., IT landscapes). The collected data were analyzed qualitatively (Myers 2013; Walsham 1993).

In a first step, a definition for rebound effects in cloud computing was derived based on the concept matrix resulting from the literature analysis and the results of the case study:

*A rebound effect in cloud computing describes the unrealized [(over)exhausted] saving of an organizational resource in consequence of a (unintentional) growth in consumption, whereas the savings could have been expected and would have been possible based on the efficiency improvement resulting from the use of cloud computing services. The organizational assessment of the effect is depending on the corporate objectives. A distinction is made between direct and indirect cloud computing rebound effects, which affect the micro- as well as macro-level in the short- or long-term.*

In summary, a rebound effect in cloud computing (RECC) can be viewed as unrealized savings of an organizational resource caused by efficiency improvements, which arise from the adoption of cloud computing services as well as from (unintended) effects on (other) organizational resources. However, a mathematical and an organizational viewpoint need to be distinguished, as it may be the case that a mathematically calculated rebound effect does not or only partially or disproportionately affect corporate objectives. The components and characteristics of a RECC are synthesized in a conceptual model (see Figure 13).

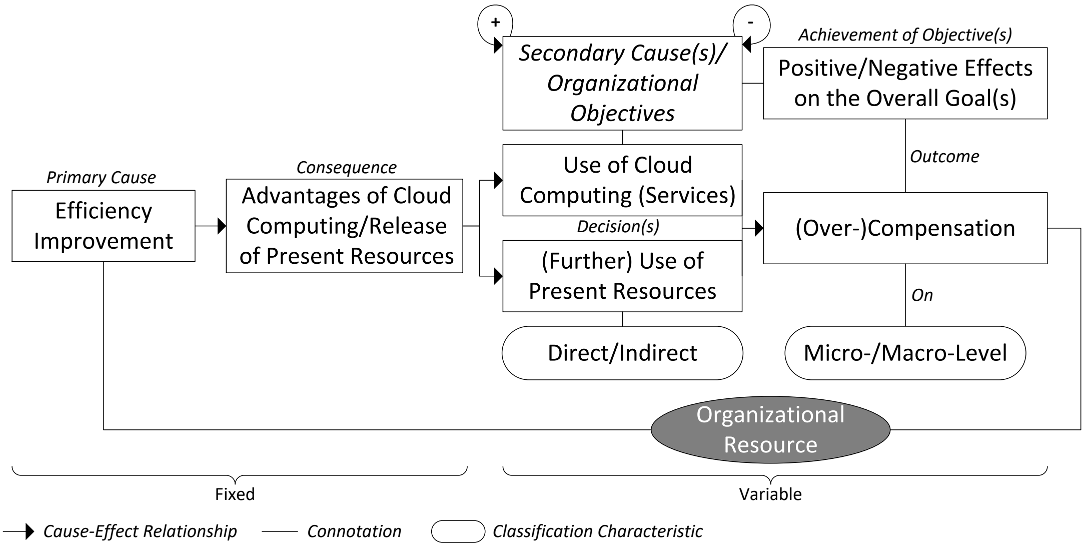
+
-
Secondary Cause(s)/ Organizational Objectives
Achievement of Objective(s)
Positive/Negative Effects on the Overall Goal(s)
Primary Cause
Efficiency Improvement
Consequence
Advantages of Cloud Computing/Release of Present Resources
Use of Cloud Computing (Services)
Decision(s)
(Further) Use of Present Resources
Outcome
(Over-)Compensation
On
Direct/Indirect
Micro-/Macro-Level
Organizational Resource
Fixed
Variable
Cause-Effect Relationship
Connotation
Classification Characteristic

Figure 13. Conceptual Model of a Rebound Effect in Cloud Computing (Adelmeyer, Walterbusch, Biermanski, et al. 2017a)

In a second step, potentially affected organizational resources were identified in the case study, which can be categorized into IT-related, hardware & systems, and general resources. Furthermore, the expected effects on organizational resources were identified and evaluated in expert workshops. The major organizational resource that is expected to be affected are financial resources (Adelmeyer, Walterbusch, Biermanski, et al. 2017b). However, the expected effects have to be assessed depending on the overall organizational goals, since, for example, a loss of employees might lead to a loss of know-how, which might contradict the goal of organizational independency.

In the study, the narrow energy saving perspective of rebound effects dominating the literature (Andrae 2013; Sedlacko et al. 2014; Walnum and Andrae 2016) was expanded by an organizational perspective (Hilty 2008). As a result, the case study showed that potential RECC can arise in any organizational area in which outsourcing into a cloud is expected to result in resource savings. The presented RECC framework, which consists of a definition, a conceptual model, and a morphological analysis, provides a foundation for the identification, categorization and understanding of potential rebound effects arising from cloud computing adoptions and their corresponding risks for organizational resources.

# 4 Discussion of the Results

## 4.1 Implications for Research and Practice

In the consecutive research contributions of this cumulative dissertation, individual research gaps were identified and addressed. In the course of the research project, a multi-method approach was chosen to investigate the research gaps in the IT security risk management of cloud services in CIs from different perspectives. The overarching intention of the thesis is to contribute to a secure integration and an adequate risk management of cloud computing services in CIs in compliance with relevant regulations, requirements, and business conditions. In addition to the theoretical contributions and the implications for theory generation, action recommendations, requirements catalogues, specifications, frameworks, models, and prototypes for practice were derived on the basis of the obtained findings. On the one hand, the practical implications aim at CI providers that want to outsource business functions or processes to cloud services and, on the other hand, at cloud service providers that want to successfully position their services in the market. Regarding the overarching intention and RQs of the thesis (see Section 1.2, RQs 1-5), each research contribution contains individual implications for theory and practice, which are jointly summarized in the following.

In Contribution A, the status quo of cloud computing adoption in CIs (RQ 1) and a research agenda were derived on the basis of a literature analysis, a practical analysis, and expert interviews. Both results constitute possible starting points for researchers and thus promote future knowledge generation. The study revealed that despite the extensive coverage of cloud service adoption in the literature only few publications focus on a CI perspective. As a central research gap, the missing consideration of national legislations and individual cloud adoption scenarios when managing cloud-related risks in CIs has been identified. The examination of this gap is essential to enable an adequate IT security risk management of cloud services in CIs. Further, the role of trust in the CI and cloud provider interaction was found to be of critical importance. In addition, jurisdictional research gaps, such as cloud-related requirements of national laws or a legally compliant adoption of cloud services were identified. For CI and cloud providers alike, the results are valuable to sustainably decide for or against the adoption of cloud services or to consider the respective research gaps and requirements when providing cloud services on the market. The research gaps identified in Contribution A further constitute the foundation for the following contributions included in this dissertation. However, due to the extensiveness of the findings, the research agenda is only partially covered, primarily focusing on the aforementioned IT security risk related research propositions without a further consideration of, e.g., technical issues. One of the identified gaps is the lack of knowledge and understanding regarding the cloud-related requirements of national CI laws. To address this gap, in Contribution B, the IT Security Law and relevant literature were analyzed to derive action recommendations, which are mainly directed at CI providers. In addition to a compact identification of the central components and implications, the effects and short-term requirements of the law were discussed. Although the implications of Contribution B are primarily of practical relevance, the findings also contribute to broadening the theoretical knowledge base of the impacts of the IT Security Law by laying the foundations for RQ 2 and motivating the need for an adequate management of IT security and related risks.

Contribution C can be regarded as the central contribution concerning the IT security risk management of cloud services from an organizational perspective (RQ 2). In Contributions B and C, the previously unchallenged exploration of the implications of the IT Security Law for cloud computing services was focused from an organizational perspective to generate an increased knowledge in this field. In expert interviews, practical knowledge was raised and hence made accessible for science by synthesizing the findings from the literature and the interviews into a requirements catalogue and, subsequently, an integrated risk management framework for CIs. Both artifacts generate implications for theory and practice alike, as they approach an urgent practical problem based on scientific methods. For CI and cloud providers, the extracted requirements and the framework can be either considered and integrated into an existing internal IT security risk management or provide the foundation for its establishment. Further, the results foster a holistic IT security risk management approach by covering the entire risk management process, cloud lifecycle, and resulting requirements. The requirements catalogue and the framework constitute the main scientific implications of Contribution C. Additionally, proactive action recommendations for CI and cloud providers were deduced based on the requirements analysis of the IT Security Law and the expert interviews. The results can further aid cloud computing providers in the strategical alignment of their services.

In Contributions D, E, and F, behavioral theories were applied in the exploration of the IT security risk management of cloud services in CIs. In this context, hypotheses were derived to investigate the role of trust and to formulate recommendations based on the extended findings. In the sense of the multi-method approach applied in this dissertation, primarily quantitative methods were obtained to explore the role of trust in risk management (RQ 3). From a scientific perspective, the findings of Contributions D, E, and F generally confirm the importance of trust as a significant factor for the adoption and use of cloud services. Furthermore, the body of knowledge of trust in cloud environments is expanded by investigating three-part relationships between interlinked entities (i.e., end-user, mediator, and cloud provider) (Jøsang et al. 2006; Jøsang and Pope 2005) in Contribution D. In addition, the finding that it is of importance for a customer's trust whether a service is provided directly or indirectly is especially relevant for both science and practice, since cloud services are often based on adapted services of different providers (Floerecke and Lehner 2016). In this context, trust issues in direct business relationships could be mitigated by service providers by providing their services via mediators, who, in turn, need to be aware of their role as the direct contractual partner of customers and their corresponding dependency on the actions of providers. As a result, mediators need to carefully select reliable providers by, for example, regularly verifying the security measures taken by providers by demanding certifications. The role of trust in the identification of cloud providers and their associated risks was investigated in Contribution E. The results of the study indicate that the perception of different trust-influencing factors on the websites of cloud providers, such as certificates, varies in comparison to others. Based on the results, recommendations were derived for the placement of trust-influencing factors to support cloud service providers and their customers in identifying reliable services. A further implication is that service providers should not only consider subjective variables but also objective metrics when designing websites to build trust. A commonly displayed metric is the reliability of a service, which can be bound contractually in SLAs to control and monitor a provider. Thus, the effects of an augmentation of SLAs were examined in Contribution F. It could be empirically proven that the factors *Information Overload*, *Transparency*, and *Ease of Use* can be regarded as determinants of cloud users' *Trusting Beliefs*, which ultimately determine the *Intention to Use* a cloud service. Thus, cloud computing providers should follow a balanced information policy based on clearly formulated and relevant information that is made available in the SLA to foster trust in business relationships. Regarding Contributions D and F, the identified determinants and the insights gained concerning the causalities of the individual constructs represent the main scientific contribution of the studies. In addition, the uncovered key determinants of trust in correspondence with concrete recommendations and measures to build trust can help cloud providers to sustainably acquire and retain existing customers. Based on the findings, novel explanatory models can be developed. Since in Contributions D, E, and F the general viewpoints of multiple actors were taken (CIs, cloud providers, and end-customers), the results regarding trust in cloud environments can be transferred to trust in other domains, such as IT risk management or IT outsourcing.

As repeatedly emphasized in the various expert interviews, there is a need for individually adaptable risk management solutions for cloud environments. Due to their individual risk and requirements focus, this is especially true for CIs (RQ 4). Thus, following a design science approach, a prototypical framework for data analyses in cloud environments was developed in Contribution G. Based on 16 expert interviews, the potential, challenges, and requirements of such a solution were examined, which constitute the main theoretical implication of this study. Additionally, the results were synthesized into a cloud architecture, which can be adapted by CI and cloud providers for extensive data analyses in each stage of risk management. To support the entire risk management process, a risk management tool for cloud services was developed in Contribution H. As a result of the iterative design science approach based on expert interviews, literature analyses, and qualitative analyses of standards and existing tools, several artifacts were generated, i.e., a requirements catalogue, use cases, technical specifications, a database model, and a software prototype. The prototype can be adapted by CI and cloud service providers to support the internal risk management of a cloud service in compliance with the individual cloud characteristics and the corresponding risks and requirements (Pearson 2013; Weintraub and Cohen 2016; Zissis and Lekkas 2012). For science, the extracted requirements, use cases, technical specifications, and the database model can be adapted for future research projects in the field of cloud risk management. Additionally, since existing cloud risk management approaches often do not holistically support risk management (Damenu and Balakrishna 2015) or do not adequately address the monitoring of controls and measures (Drissi et al. 2013), the prototype extends the existing body of knowledge in cloud risk management.

A further implication for science of Contribution H is the extensive list of risks in cloud service environments (RQ 5), which was derived based on the literature analysis and the expert interviews from a general perspective. Out of these risks, the general fields of data security and privacy were examined in detail in Contribution I. The core contribution of the study – a framework for the evaluation of data security and privacy in cloud services – is of both practical and theoretical value. The framework can be adapted by CIs, cloud providers or third-party organizations, such as auditing or consulting companies, to determine data security and data privacy measures and controls of cloud services. The sub-models of the framework reflect general implications and guidance for theory and practice and need to be adapted individually. Therefore, the role of privacy and security is examined in the exemplary critical industry sector of healthcare in Contribution J, in which the impacts of the storage location and data breaches on end-customers are examined. The experiment revealed that the *Perceived Security* and *Perceived Privacy* are largely determined by the *Trust* and the *Perceived Control* of a subject, which ultimately determine the *Intention to Use* a service. In addition, the fact that the subjects' *Perceived Security, Perceived Privacy, Perceived Control,* and *Trust* are significantly higher when data are stored on-premise urges PHR providers to decide whether to offer their services in cloud environments or on-premise. However, after a data breach, the subjects' attitudes towards privacy and security regarding cloud and on-premise hosting do not differ significantly. Therefore, security and privacy measures need to be emphasized by PHR and cloud service providers to foster the trust of (potential) customers, e.g., by providing transparency via certifications, which are re-audited on a regular basis (Sunyaev and Schneider 2013). PHR providers might consider private clouds to minimize concerns regarding security and privacy on the users' side. To realize cloud-related benefits and economies of scale, hybrid cloud environments can be used for encrypted or non-sensitive data. As an exemplary economic risk factor, rebound effects were examined in an exploratory case study in Contribution K. The resulting framework, consisting of a definition, a conceptual model, and a morphological analysis of rebound effects, provides the basis for further research on the previously unchallenged phenomenon. Since efficiency benefits are regarded as major driving factor of cloud computing adoption (Armbrust et al. 2010; Marston et al. 2011), the understanding of influences and effects endangering organizational resources and ultimately the targeted benefits is crucial. Further, corporate decision makers need to be aware that the decision to adopt cloud services and the resulting effects might partially contradict organizational goals. In summary, the identification, categorization, and understanding of the potential rebound effects in cloud computing is vital for organizations for a sustainable judgement whether to adopt cloud services in critical infrastructures.

## 4.2 Limitations and Future Research

Regarding the limitations of the dissertation project, two levels have to be distinguished. On the macro level, limitations concerning the overall scope and approach of the dissertation need to be outlined, whereas on the micro level, the limitations associated with the individual methods applied in the selected research contributions are focused. On the one hand, the limitations should be taken into account when interpreting the results. On the other hand, they also mark future research opportunities. The paper-specific limitations are discussed comprehensively in the individual research contributions in Part B. The limitations of the overall research approach at the macro level together with future research opportunities and the core limitations of the research methods applied at the micro level (see Section 2.2) are summarized below.

At the macro level, several limitations and opportunities for future research need to be highlighted. When applying a multi-method approach, researchers are confronted with the challenge of obtaining a meaningful balance and weighting of the methods used (Venkatesh et al. 2013). Although a certain balance between qualitative and quantitative research methods has been maintained in this dissertation, qualitative methods take a significant share. Therefore, further quantitative examinations might be integrated where reasonable. Regarding the research framework (see Section 2.3), a distinction between the service and deployment models of cloud computing has not been made. However, since the risks associated with the adoption of cloud services vary considerably between the selected cloud service and deployment models (Adelmeyer and Teuteberg 2018a), a further differentiated analysis of the cloud-related risks and risk management for individual cloud adoption scenarios is necessary. Furthermore, only exemplary risks could be examined at an aggregated level, without considering industry- or organization-specific factors. Thus, further studies focusing on the technical aspects of concrete IT security risks would provide a valuable complementation of the results of this dissertation.

The perspectives taken in this dissertation constitute a further limitation. Since the IT security risk management of cloud services in CIs was primarily examined from an organizational and legal perspective concentrating on the integration of risk management processes and the overall compliance with legal requirements, concrete technical implications could not be focused. Furthermore, a formal mathematical consideration of cloud-related risks is missing. This includes both a quantitative examination of the risk probabilities and risk measures as well as a monetary perspective. In line with the research agenda formulated in Contribution A, starting points for future research are the technical issues and implications related to the IT security risk management of cloud usage in CIs, such as hybrid cloud frameworks for CIs or the secure deployment of critical business functions in public clouds. Regarding the legal perspective, constant regulatory amendments concerning the IT security and privacy of IT systems fuel the need for a continuous adjustment of IT security and risk management measures. Additionally, the research domain was mainly approached from the perspective of either cloud service providers or cloud service users, i.e., CIs. However, further stakeholders exist that need to be considered when outsourcing critical functions or processes to a cloud, such as legislators, standard developers, customers or technology providers (Floerecke and Lehner 2016; Keller and König 2014). In essence, the dissertation provides fundamental implications for CIs and cloud service providers regarding the IT security risk management of cloud services, which need to be individually adapted to the respective cloud usage scenario.

At the micro level, various limitations need to be considered. Regarding the systematic literature reviews that were either conducted as a theoretical foundation or as an exploration of a research field in each research contribution, several possible limitations arise. Although the selection and the analysis of relevant publications were conducted in compliance with generally accepted procedures (e.g., vom Brocke et al. 2009; Webster and Watson 2002), limitations may arise. These are based on various factors, such as the restriction to a certain scope of publications, the selection of certain search terms, or possibly unidentified publications. Furthermore, the qualitative analysis of the relevant research contributions potentially leads to a bias of the results. In addition, since Contributions B, C, and I focused on national legislation and therefore predominantly consult German literature, the generalizability of the results is partially limited.

Similar limitations arise regarding the execution of the expert interviews in Contributions A, C, G, H, I, and K. The interviews were mainly conducted with experts from Germany, which is primarily due to the subject of the study and the availability of qualified experts. Furthermore, the coding of the expert interviews as part of the qualitative analysis might be biased by the individual expectations and backgrounds of a researcher. Therefore, the coding was always carried out or reviewed by multiple researchers to avoid possible misinterpretations. Furthermore, expert interviews represent the main data source for the research results in Contributions C, G, and I, which is why further evaluation is desirable.

The case study conducted in Contribution K followed the approach of a single case study setup. Single case study setups are particularly suitable for the examination of unchallenged phenomena at the beginning of theory generation (Recker 2013), which coincides with the research objective to describe rebound effects in cloud computing. However, multiple case setups allow for a cross-case validation of theories and therefore generate more reliable results (Darke et al. 1998; Recker 2013). In addition, the overall generalizability of the results and conclusions drawn from case study approaches beyond the investigated cases is discussed critically (Dubé and Paré 2003; Gable 1994). To address the limitations of case study research, Contribution K fundamentally follows the elements and procedures of the established and recognized guidelines of Dubé and Paré (2003), Gable (1994), Newell and Simon (1972) and Recker (2013). Nevertheless, future research projects could examine additional organizations and focus on the investigation of RECCs in other industrial sectors by applying quantitative research methods.

The prototypical framework for data analyses in clouds developed in Contribution G was not practically applied. Consequently, the practical validity and applicability of the framework have to be confirmed. Regarding the prototyping conducted in Contribution H, only one application version was evaluated externally. Here, in accordance with the design science principle applied, further iterations of the generate/test cycle including further external evaluations are desirable (Hevner et al. 2004). Since the goal of the research endeavor is to continuously improve the solution to eventually make it publicly available, a previous prototypical implementation and adaption of the solution in the field is advised.

Experimental setups (Contributions D, F, and J) or web-based surveys (Contributions E and H) suffer from several limitations. First, conducting experiments with student participants, as was done in Contributions D, F, and J, is a controversial topic (Compeau et al. 2012). However, as students' technology adoption and usage decisions do not differ significantly from others (McKnight et al. 2011; Sen et al. 2006) and they are deemed early adopters of innovative technologies (Gallagher et al. 2001), such as cloud computing, they constitute an adequate target sample for the studies conducted. Second, the applied vignette survey approach is based on a fictitious environment, in which the participants are asked to put themselves in an organizational context. Therefore, it is possible that the participants did not behave as they would in a real environment (Aguinis and Bradley 2014; Greenberg and Eskew 1993). Third, the overall limitations of web-based experimenting apply (Reips 2002). In essence, a generalization of the experiment results to other geographical regions or subjects should be made with caution, since theoretical constructs, such as trust or perceived privacy, might be influenced by the respective cultural or national context (Leidner and Kayworth 2006). Therefore, future research should aim to replicate the results with different samples. In Contribution D, only unidirectional trust relationships from the end-users' perspective were examined, although each trust relationship is of bidirectional nature (Adelmeyer, Walterbusch, et al. 2018). Further, different trust targets exist in the context of cloud computing (Söllner et al. 2016), such as the trust in the technology itself. However, the focus of Contributions D, E, F, and J was put on the trust in a service provider. As student participants were consulted for the experiments from the end-users' perspective, the limited generalizability for organizational contexts needs to be considered.

A major limitation of the eye-tracking study conducted in Contribution E is the interpretation of the results. Since gaze recordings measure the total fixations of a subject on a certain area of interest, an understanding of the context is necessary. The total fixations recorded can indicate both stimulus properties (complexity) and recipient properties (interest) (Blake 2013; Duchowski 2007). Thus, the interpretation of the number of fixations only permits limited conclusions regarding the effect on recipients. To overcome this limitation, the results of the gaze recordings were combined with data from a subsequent survey, in which the individual attitudes of the participants were collected.

# 5 Conclusion

The objective of this doctoral thesis was to examine the IT security risk management of cloud services in CIs. For this purpose, frameworks, conceptual models, prototypical tools, action recommendations, and implications were developed both for science and practice. In this context, five overarching research questions were formulated (see Section 1.2). Within the scope of the eleven research contributions included in this doctoral thesis (see Section 2.1), the various RQs were examined. The status quo of cloud computing service adoption in German critical infrastructures and the corresponding research gaps were determined in Contribution A (RQ 1). Implications and methods for an adequate management of IT security and the corresponding risks resulting from the adoption of cloud computing services were derived in Contributions B and C (RQ 2). In the context of the interaction between CI and cloud computing service providers, the role of trust was examined in Contributions D, E, and F (RQ 3). In Contributions G and H, frameworks and prototypes for a tool support for the IT security risk management of cloud services in CIs were developed (RQ 4). The risks resulting from the adoption of cloud computing services were examined in Contributions H, I, J, and K (RQ 5). All contributions have been published in prestigious conference proceedings and renowned journals to promote the transfer of the research results.

As an underlying analytical framework, a multi-method approach was chosen to examine the field from a behavioral- as well as a design-oriented perspective by applying various qualitative and quantitative research methods (see Section 2.2). Following the focus of the research questions, the framework of the research contributions (see Section 2.3) was divided into three main perspectives, i.e., the status quo and research agenda of cloud adoption in CIs, the IT security risk management of cloud computing services in CIs, which follows a typical risk management process, and the cloud-related IT security risk factors.

In summary, critical and relevant questions from IT practice have been examined with recognized scientific methods and established theories. The findings contribute to the body of knowledge of both science and practice. Further, the results of this dissertation can significantly support the IT security risk management of cloud computing services in CIs. However, the dissertation does not claim to fully cover the extensiveness and complexity of the field, since, for example, the requirements and risks vary between the individual CI sectors and cloud adoption scenarios and therefore require an individual examination (Adelmeyer, Petrick, et al. 2018). In addition, as a complete coverage of the identified research gaps in

Contribution A was not possible within the boundaries of this dissertation, a further need for research exists. Nevertheless, the presented results are helpful to substantially support decision makers and researchers in the field of the IT security risk management of cloud services in CIs.

# References

Ackermann, T. 2013. *IT Security Risk Management*, Wiesbaden, Germany: Springer Gabler.

Adelmeyer, M., Beike, L., Buggenthin, M., Osada, S., and Teuteberg, F. 2018. "RisCC – A Risk Management Tool for Cloud Computing Environments," in *Proceedings of the 24th Americas Conference on Information Systems (AMCIS 2018)*, New Orleans, LA, USA.

Adelmeyer, M., Beinke, J. H., Walterbusch, M., Gameiro, R. R., König, P., and Teuteberg, F. 2016. "Eye-Tracking zur Untersuchung von Vertrauenssignalen auf Webseiten von Cloud Computing-Anbietern," in *Proceedings of the 46. Jahrestagung der Gesellschaft für Informatik (INFORMATIK 2016)*, Lecture Notes in Informatics, Klagenfurt, Austria, pp. 883–896.

Adelmeyer, M., Meier, P., and Teuteberg, F. 2019. "Security and Privacy of Personal Health Records in Cloud Computing Environments – An Experimental Exploration of the Impact of Storage Solutions and Data Breaches," in *Proceedings of the 14th International Conference on Wirtschaftsinformatik (WI 2019)*, Siegen, Germany, pp. 912–926.

Adelmeyer, M., Petrick, C., and Teuteberg, F. 2017. "IT-Risikomanagement von Cloud-Dienstleistungen im Kontext des IT-Sicherheitsgesetzes," *HMD – Praxis der Wirtschaftsinformatik* (54:1), pp. 111–123.

Adelmeyer, M., Petrick, C., and Teuteberg, F. 2018. *IT-Risikomanagement von Cloud-Services in Kritischen Infrastrukturen*, Wiesbaden, Germany: Springer Vieweg.

Adelmeyer, M., and Teuteberg, F. 2016. "Cloud-Architekturen für Datenanalysen in Wirtschaftsprüfungsgesellschaften," *HMD – Praxis der Wirtschaftsinformatik* (53:5), pp. 698–711.

Adelmeyer, M., and Teuteberg, F. 2018a. "Cloud Computing Adoption in Critical Infrastructures – Status Quo and Elements of a Research Agenda," in *Proceedings zur Multikonferenz Wirtschaftsinformatik (MKWI 2018)*, Lüneburg, Germany, pp. 1345–1356.

Adelmeyer, M., and Teuteberg, F. 2018b. "Datenanalysen in der Cloud – Konzeption einer Architektur für die Wirtschaftsprüfung," in *Cloud Computing*, S. Reinheimer (ed.), Wiesbaden, Germany: Springer Fachmedien, pp. 89–102.

Adelmeyer, M., Walterbusch, M., Biermanski, P., Seifert, K., and Teuteberg, F. 2017a. "Rebound Effects in Cloud Computing: Towards a Conceptual Framework," in *Proceedings of the 13th International Conference on Wirtschaftsinformatik (WI 2017)*, St. Gallen, Switzerland, pp. 499–513.

Adelmeyer, M., Walterbusch, M., Biermanski, P., Seifert, K., and Teuteberg, F. 2017b. "Rebound-Effekte im Cloud Computing," *HMD – Praxis der Wirtschaftsinformatik* (54:3), pp. 389–402.

Adelmeyer, M., Walterbusch, M., Biermanski, P., and Teuteberg, F. 2018. "Trust Transitivity and Trust Propagation in Cloud Computing Ecosystems," in *Proceedings of the 26th European Conference on Information Systems (ECIS 2018)*, Portsmouth, UK.

Adelmeyer, M., Walterbusch, M., Lang, J., and Teuteberg, F. 2017. "Datenschutz und Datensicherheit im Cloud Computing – Ein Framework zur Beurteilung von Cloud-Services," *Die Wirtschaftsprüfung (WPg)* (70:1), pp. 35–42.

Adelmeyer, M., Walterbusch, M., Seifert, K., and Teuteberg, F. 2016. "Does the Augmentation of Service Level Agreements Affect User Decisions in Cloud Adoption Scenarios? – An Experimental Approach," in *Proceedings of the 24th European Conference on Information Systems (ECIS 2016),* Istanbul, Turkey.

Aguinis, H., and Bradley, K. J. 2014. "Best Practice Recommendations for Designing and Implementing Experimental Vignette Methodology Studies," *Organizational Research Methods* (17:4), pp. 351–371.

Alchian, A. A., and Demsetz, H. 1972. "Production, Information Costs, and Economic Organization," *The American Economic Review* (62:5), pp. 777–795.

Andrae, A. S. G. 2013. "Comparative Micro Life Cycle Assessment of Physical and Virtual Desktops in a Cloud Computing Network with Consequential, Efficiency, and Rebound Considerations," *Journal of Green Engineering* (3:2), pp. 193–218.

Armbrust, M., Fox, A., Griffith, R., Joseph, A. D., Katz, R., Konwinski, A., Lee, G., Patterson, D., Rabkin, A., Stoica, I., and Zaharia, M. 2010. "A View of Cloud Computing," *Communications of the ACM* (53:4), pp. 50–58.

Aronson, E., and Carlsmith, J. M. 1968. "Experimentation in Social Psychology," in *Handbook of Social Psychology,* G. Lindzey and E. Aronson (eds.), Reading, MA, USA: Addison Wesley, pp. 1–79.

Baldwin, A., Pym, D., and Shiu, S. 2013. "Enterprise Information Risk Management: Dealing with Cloud Computing," in *Privacy and Security for Cloud Computing,* S. Pearson and G. Yee (eds.), London: Springer, pp. 257–291.

Benbasat, I., Goldstein, D. K., and Mead, M. 1987. "The Case Research Strategy in Studies of Information Systems," *MIS Quarterly* (11:3), pp. 369–386.

Benlian, A., and Hess, T. 2011. "The Signaling Role of IT Features in Influencing Trust and Participation in Online Communities," *International Journal of Electronic Commerce* (15:4), pp. 7–56.

Blake, C. 2013. "Eye-Tracking: Grundlagen und Anwendungsfelder," in *Handbuch standardisierte Erhebungsverfahren in der Kommunikationswissenschaft,* W. Möhring and D. Schlütz (eds.), Wiesbaden, Germany: Springer, pp. 367–387.

Bless, R., Hutchison, D., Schöller, M., Smith, P., and Tauber, M. 2013. "SECCRIT: Secure Cloud Computing for High Assurance Services," *ERCIM NEWS* (95), pp. 40–41.

Bojko, A. 2009. "Informative or Misleading? Heatmaps Deconstructed," in *Proceedings of the 13th International Conference on Human-Computer Interaction (HCII 2009),* San Diego, CA, USA.

Bonoma, T. V. 1985. "Case Research in Marketing: Opportunities, Problems, and a Process," *Journal of Marketing Research* (22:2), pp. 199–208.

vom Brocke, J., Simons, A., Niehaves, B., Riemer, K., Plattfaut, R., and 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),* Verona, Italy.

Catteddu, D., and Hogben, G. 2009. "Cloud Computing – Benefits, Risks and Recommendations for Information Security," *ENISA Reports,* Heraklion, Greece: European Network and Information Security Agency (ENISA).

Chin, W. W. 1998a. “Issues and Opinion on Structural Equation Modeling Clear Reporting,” *MIS Quarterly* (22:1), pp. vii–xvi.

Chin, W. W. 1998b. “The Partial Least Squares Approach for Structural Equation Modeling,” in *Modern Methods for Business Research*, G. A. Marcoulides (ed.), Mahwah, New Jersey, USA: Lawrence Erlbaum, pp. 295–336.

Chochliouros, I. P., Spiliopoulou, A. S., Stephanakis, I. M., Arvanitozisis, D. N., Sfakianakis, E., Belesioti, M., Georgiadou, E., and Mitsopoulou, N. 2015. “Security and Protection of Critical Infrastructures: A Conceptual and Regulatory Overview for Network and Information Security in the European Framework, also Focusing upon the Cloud Perspective,” in *Proceedings of the 16th International Conference on Engineering Applications of Neural Networks (EANN 2015)*, Rhodes Island, Greece.

Clemons, E. K., and Chen, Y. 2011. “Making the Decision to Contract for Cloud Services: Managing the Risk of an Extreme Form of IT Outsourcing,” in *Proceedings of the 44th Hawaii International Conference on System Sciences (HICSS 2011)*, Kauai, HI, USA.

Compeau, D., Marcolin, B., Kelley, H., and Higgins, C. 2012. “Research Commentary: Generalizability of Information Systems Research Using Student Subjects – A Reflection on our Practices and Recommendations for Future Research,” *Information Systems Research* (23:4), pp. 1093–1109.

Cooper, D. R., and Schindler, P. S. 2014. *Business Research Methods*, New York, NY, USA: McGraw-Hill.

Creswell, J. W., and Creswell, J. D. 2018. *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches*, Thousand Oaks, CA, USA: Sage.

Damenu, T. K., and Balakrishna, C. 2015. “Cloud Security Risk Management: A Critical Review,” in *Proceedings of the 9th International Conference on Next Generation Mobile Applications, Services and Technologies (NGMAST 2015)*, Cambridge, UK, pp. 370–375.

Darke, P., Shanks, G., and Broadbent, M. 1998. “Successfully Completing Case Study Research: Combining Rigour, Relevance and Pragmatism,” *Information Systems Journal* (8:4), pp. 273–289.

Das, T. K., and Teng, B.-S. 2004. “The Risk-Based View of Trust: A Conceptual Framework,” *Journal of Business and Psychology* (19:1), pp. 85–116.

Davis, A. M. 1992. “Operational Prototyping: A New Development Approach,” *IEEE Software* (9:5), pp. 70–78.

Dekker, M. A. C. 2012. “Critical Cloud Computing,” *ENISA Reports*, Heraklion, Greece: European Network and Information Security Agency (ENISA).

Diez, O., and Silva, A. 2011. “Reliability Issues Related to the Usage of Cloud Computing in Critical Infrastructures,” in *Proceedings of the 20th European Safety and Reliability Conference (ESREL 2011)*, Troyes, France.

Djemame, K., Armstrong, D. J., Kiran, M., and Jiang, M. 2011. “A Risk Assessment Framework and Software Toolkit for Cloud Service Ecosystems,” in *Proceedings of the 2nd International Conference on Cloud Computing, GRIDs, and Virtualization (CLOUD COMPUTING 2011)*, Rome, Italy, pp. 119–126.

Drissi, S., Houmani, H., and Medromi, H. 2013. “Survey: Risk Assessment for Cloud Computing,” *International Journal of Advanced Computer Science and Applications* (4:12), pp. 143–148.

Dubé, L., and Paré, G. 2003. "Rigor in Information Systems Positivist Case Research: Current Practices, Trends, and Recommendations," *MIS Quarterly* (27:4), pp. 597–635.

Duchowski, A. 2007. *Eye Tracking Methodology*, London, UK: Springer.

Earle, T. C. 2010. "Trust in Risk Management: A Model-Based Review of Empirical Research," *Risk Analysis* (30:4), pp. 541–574.

Eckert, C. 2018. *IT-Sicherheit*, Berlin, Germany: Walter de Gruyter.

European Council. 2008. "Council Directive 2008/114/EC of 8 December 2008 on the Identification and Designation of European Critical Infrastructures and the Assessment of the Need to Improve their Protection," (available at http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32008L0114; retrieved October, 31, 2019).

Finch, J. 1987. "The Vignette Technique in Survey Research," *Sociology* (21:1), pp. 105–114.

Fishbein, M., and Ayzen, I. 1975. *Belief, Attitude, Intention and Behavior: An Introduction to Theory and Research*, Reading, MA, USA: Addison-Wesley.

Floerecke, S., and Lehner, F. 2016. "Cloud Computing Ecosystem Model: Refinement and Evaluation," in *Proceedings of the 24th European Conference on Information Systems (ECIS 2016)*, Istanbul, Turkey.

Florian, M., Paudel, S., and Tauber, M. 2013. "Trustworthy Evidence Gathering Mechanism for Multilayer Cloud Compliance," in *Proceedings of the 8th International Conference for Internet Technology and Secured Transactions (ICITST 2013)*, London, UK, pp. 529–530.

Gable, G. G. 1994. "Integrating Case Study and Survey Research Methods: An Example in Information Systems," *European Journal of Information Systems* (3:2), pp. 112–126.

Gallagher, K., Parsons, J., and Foster, K. D. 2001. "A Tale of Two Studies: Replicating 'Advertising Effectiveness and Content Evaluation in Print and on the Web'," *Journal of Advertising Research* (41:4), pp. 71–81.

Gläser, J., and Laudel, G. 2010. *Experteninterviews und qualitative Inhaltsanalyse*, Wiesbaden, Germany: Springer VS Verlag für Sozialwissenschaften.

Goldshteyn, M., and Adelmeyer, M. 2015. "Die Auswirkungen des IT-Sicherheitsgesetzes auf die Interne Revision," *Zeitschrift Interne Revision* (50:6), pp. 244–255.

Gossart, C. 2014. "Rebound Effects and ICT : A Review of the Literature," in *ICT Innovations for Sustainability*, L. M. Hilty and B. Aebischer (eds.), Cham, Switzerland: Springer, pp. 435–448.

Greenberg, J., and Eskew, D. E. 1993. "The Role of Role Playing in Organizational Research," *Journal of Management* (19:2), pp. 221–241.

Hecht, T., Smith, P., and Schöller, M. 2014. "Critical Services in the Cloud: Understanding Security and Resilience Risks," in *Proceedings of the 6th International Workshop on Reliable Networks Design and Modeling (RNDM 2014)*, Barcelona, Spain, pp. 131–137.

Heinzl, A., Schoder, D., and Frank, U. 2008. "WI-Journalliste 2008 sowie WI-Liste der Konferenzen, Proceedings und Lecture Notes 2008," *Wirtschaftsinformatik* (50:2), pp. 155–163.

Hevner, A. 2007. "A Three Cycle View of Design Science Research," *Scandinavian Journal of Information Systems* (19:2), pp. 87–92.

Hevner, A., March, S. T., Park, J., and Ram, S. 2004. “Design Science in Information Systems Research,” *MIS Quarterly* (28:1), pp. 75–105.

Hilty, L. M. 2008. *Information Technology and Sustainability,* Norderstedt, Germany: Books on Demand.

Holmqvist, K., Nyström, M., Andersson, R., Dewhurst, R., Jarodzka, H., and van de Weijer, J. 2011. *Eye Tracking: A Comprehensive Guide to Methods and Measures*, Oxford, UK: Oxford University Press.

Hudic, A., Hecht, T., Tauber, M., Mauthe, A., and Santiago Cáceres, E. 2014. “Towards Continuous Cloud Service Assurance for Critical Infrastructure IT,” in *Proceedings of the 2nd International Conference on Future Internet of Things and Cloud (FiCloud 2014),* Barcelona, Spain, pp. 175–182.

Jenkins, A. M. 1985. “Research Methodologies and MIS Research,” in *Research Methods in Information Systems,* E. Mumford, R. A. Hirschheim, G. Fitzgerald, and A. T. Wood-Harper (eds.), Amsterdam, Netherlands: North-Holland, pp. 103–117.

Jensen, M., and Meckling, W. 1976. “Theory of the Firm: Managerial Behavior, Agency Costs and Ownership Structure,” *Journal of Financial Economics* (3:4), pp. 305–360.

Jick, T. D. 1979. “Mixing Qualitative and Quantitative Methods: Triangulation in Action,” *Administrative Science Quarterly* (24:4), pp. 602–611.

Jøsang, A., Hayward, R., and Pope, S. 2006. “Trust Network Analysis with Subjective Logic,” in *Proceedings of the 29th Australasian Computer Science Conference (ACSC 2006),* Hobart, Australia, pp. 85–94.

Jøsang, A., and Pope, S. 2005. “Semantic Constraints for Trust Transitivity,” in *Proceedings of the 2nd Asia-Pacific Conference on Conceptual Modelling (APCCM 2005),* Newcastle, Australia, pp. 59–68.

Kandel, E. R., Schwartz, J. H., Jessell, T. M., Siegelbaum S. A., and Hudspeth, A. J. 2012. *Principles of Neural Science*, New York, NY, USA: McGraw-Hill.

Kaplan, B., and Duchon, D. 1988. “Combining Qualitative and Quantitative Methods in Information Systems Research: A Case Study,” *MIS Quarterly* (12:4), pp. 571–586.

Kaplan, B., and Maxwell, J. A. 1994. “Qualitative Research Methods for Evaluating Computer Information Systems,” in *Evaluating Health Care Information Systems: Methods and Applications*, J. G. Anderson, C. E. Aydin, and S. J. Jay (eds.), Thousand Oaks, CA, USA: Sage, pp. 45–68.

Keller, R. 2016. “Analyse von Risikomanagementstrategien in Cloudnetzwerken – Was tun bei verknüpften, voneinander abhängigen Cloud Services?,” *HMD – Praxis der Wirtschaftsinformatik* (53:5), pp. 674–687.

Keller, R., and König, C. 2014. “A Reference Model to Support Risk Identification in Cloud Networks,” in *Proceedings of the 35th International Conference on Information Systems (ICIS 2014),* Auckland, NZ.

Klipper, S. 2015. *Information Security Risk Management: Risikomanagement mit ISO/IEC 27001, 27005 und 31010*, Wiesbaden, Germany: Springer Vieweg.

Königs, H.-P. 2017. *IT-Risikomanagement mit System,* Wiesbaden, Germany: Springer.

Kushida, K. E., Murray, J., and Zysman, J. 2011. “Diffusing the Cloud: Cloud Computing and Implications for Public Policy,” *Journal of Industry, Competition and Trade* (11:3), pp. 209–237.

Lansing, J., and Sunyaev, A. 2016. "Trust in Cloud Computing: Conceptual Typology and Trust-Building Antecedents," *ACM SIGMIS Database* (47:2), pp. 58–96.

Leidner, D. E., and Kayworth, T. 2006. "A Review of Culture in Information Systems Research: Toward a Theory of Information Technology Culture Conflict," *MIS Quarterly* (30:2), pp. 357–399.

Leimeister, S., Böhm, M., Riedl, C., and Krcmar, H. 2010. "The Business Perspective of Cloud Computing: Actors, Roles, and Value Networks," in *Proceedings of the 18th European Conference on Information Systems (ECIS 2010)*, Pretoria, South Africa.

Liebold, R., and Trinczek, R. 2009. "Experteninterview," in *Handbuch Methoden der Organisationsforschung*, S. Kühl, P. Strodtholz, and A. Taffertshofer (eds.), Wiesbaden, Germany: Springer VS Verlag für Sozialwissenschaften, pp. 32–56.

Lowry, P. B., and Gaskin, J. 2014. "Partial Least Squares (PLS) Structural Equation Modeling (SEM) for Building and Testing Behavioral Causal Theory: When to Choose it and How to Use it," *IEEE Transactions on Professional Communication* (57:2), pp. 123–146.

MacDermott, A., Shi, Q., Merabti, M., and Kifayat, K. 2013. "Protecting Critical Infrastructure Services in the Cloud Environment," in *Proceedings of the 12th European Conference on Information Warfare and Security (ECCWS 2013)*, Jyväskylä, Finland, pp. 336–343.

MacDermott, A., Shi, Q., Merabti, M., and Kifayat, K. 2015. "Hosting Critical Infrastructure Services in the Cloud Environment Considerations," *International Journal of Critical Infrastructures* (11:4), pp. 365–381.

Mackay, M., Baker, T., and Al-Yasiri, A. 2012. "Security-Oriented Cloud Computing Platform for Critical Infrastructures," *Computer Law & Security Review* (28:6), pp. 679–686.

Marston, S., Li, Z., Bandyopadhyay, S., Zhang, J., and Ghalsasi, A. 2011. "Cloud Computing – The Business Perspective," *Decision Support Systems* (51:1), pp. 176–189.

Mayer, Davis, J. H., and Schoorman, F. D. 1995. "An Integrative Model of Organizational Trust," *The Academy of Management Review*, (20:3), pp. 709–734.

McKnight, D. H., Carter, M., Thatcher, J. B., and Clay, P. F. 2011. "Trust in a Specific Technology: An Investigation of its Components and Measures," *ACM Transactions on Management Information Systems* (2:2).

Mell, P., and Grance, T. 2011. "The NIST Definition of Cloud Computing," *NIST Special Publication 800-145*, National Institute of Standards and Technology (NIST).

Meuser, M., and Nagel, U. 2009. "The Expert Interview and Changes in Knowledge Production," in *Interviewing Experts*, A. Bogner, B. Littig, and W. Menz (eds.), London, UK: Palgrave Macmillan, pp. 17–42.

Myers, M. D. 2013. *Qualitative Research in Business & Management*, London, UK: Sage.

Newell, A., and Simon, H. A. 1972. *Human Problem Solving*, Englewood Cliffs, NJ, USA: Prentice-Hall.

van Niekerk, B., and Jacobs, P. 2013. "Cloud-Based Security Mechanisms for Critical Information Infrastructure Protection," in *Proceedings of the International Conference on Adaptive Science and Technology (ICAST 2013)*, Pretoria, South Africa.

Oates, B. J. 2006. *Researching Information Systems and Computing*, London, UK: Sage.

Österle, H., Becker, J., Frank, U., Hess, T., Karagiannis, D., Krcmar, H., Loos, P., Mertens, P., Oberweis, A., and Sinz, E. J. 2011. "Memorandum on Design-Oriented Information Systems Research," *European Journal of Information Systems* (20:1), pp. 7–10.

Patton, M. Q. 2015. *Qualitative Research & Evaluation Methods,* Thousand Oaks, CA, USA: Sage.

Paudel, S., Tauber, M., and Brandic, I. 2013. "Security Standards Taxonomy for Cloud Applications in Critical Infrastructure IT," in *Proceedings of the 8th International Conference for Internet Technology and Secured Transactions (ICITST 2013),* London, UK, pp. 645–646.

Paudel, S., Tauber, M., Wagner, C., Hudic, A., and Ng, W.-K. 2014. "Categorization of Standards, Guidelines and Tools for Secure System Design for Critical Infrastructure IT in the Cloud," in *Proceedings of the 6th International Conference on Cloud Computing Technology and Science (CloudCom 2014),* Singapore, Singapore, pp. 956–963.

Pavlou, P. A., Liang, H., and Xue, Y. 2007. "Understanding and Mitigating Uncertainty in Online Exchange Relationships: A Principal-Agent Perspective," *MIS Quarterly* (31:1), pp. 105–136.

Pearson, S. 2013. "Privacy, Security and Trust in Cloud Computing," in *Privacy and Security for Cloud Computing,* S. Pearson and G. Yee (eds.), London, UK: Springer, pp. 3–42.

Peffers, K., Tuunanen, T., Rothenberger, M. A., and Chatterjee, S. 2007. "A Design Science Research Methodology for Information Systems Research," *Journal of Management Information Systems* (24:3), pp. 45–77.

Piggin, R. 2015. "Are Industrial Control Systems Ready for the Cloud?," *International Journal of Critical Infrastructure Protection* (9:C), pp. 38–40.

Recker, J. 2013. *Scientific Research in Information Systems: A Beginner's Guide*, Heidelberg, Germany: Springer.

Reips, U.-D. 2002. "Standards for Internet-Based Experimenting," *Experimental Psychology* (49:4), pp. 243–256.

Ringle, C. M., Sarstedt, M., and Straub, D. W. 2012. "A Critical Look at the Use of PLS-SEM in MIS Quarterly," *MIS Quarterly* (36:1), pp. iii–xiv.

Ringle, C. M., Wende, S., and Becker, J.-M. 2015. SmartPLS 3, Bönningstedt: SmartPLS, (available at http://www.smartpls.com; retrieved October, 31, 2019).

Ross, S. A. 1977. "The Determination of Financial Structure: The Incentive-Signaling Approach," *The Bell Journal of Economics* (8:1), pp. 23–40.

Rudolph, M., Schwarz, R., and Jung, C. 2014. "Security Policy Specification Templates for Critical Infrastructure Services in the Cloud," in *Proceedings of the 9th International Conference for Internet Technology and Secured Transactions (ICITST 2014),* London, UK, pp. 61–66.

Schöller, M., Bless, R., Pallas, F., Horneber, J., and Smith, P. 2013. "An Architectural Model for Deploying Critical Infrastructure Services in the Cloud," in *Proceedings of the 5th International Conference on Cloud Computing Technology and Science (CloudCom 2013),* Bristol, UK.

Sedlacko, M., Martinuzzi, A., and Dobernig, K. 2014. "A Systems Thinking View on Cloud Computing and Energy Consumption," in *Proceedings of the 2nd International Conference on ICT for Sustainability (ICT4S 2014),* Stockholm, Sweden, pp. 95–102.

Sen, R., King, R. C., and Shaw, M. J. 2006. “Buyers’ Choice of Online Search Strategy and its Managerial Implications,” *Journal of Management Information Systems* (23:1), pp. 211–238.

Shadish, W. R., Cook, T. D., and Campbell, D. T. 2002. *Experimental and Quasi-Experimental Designs for Generalized Causal Inference*, Boston, MA, USA: Houghton Mifflin.

Sherchan, W., Nepal, S., and Paris, C. 2013. “A Survey of Trust in Social Networks,” *ACM Computing Surveys* (45:4).

Söllner, M., Hoffmann, A., and Leimeister, J. M. 2016. “Why Different Trust Relationships Matter for Information Systems Users,” *European Journal of Information Systems* (25:3), pp. 274–287.

Spence, M. 1973. “Job Market Signaling,” *The Quarterly Journal of Economics* (87:3), pp. 355–374.

Stankov, I., Datsenka, R., and Kurbel, K. 2012. “Service Level Agreement as an Instrument to Enhance Trust in Cloud Computing – An Analysis of Infrastructure-as-a-Service Providers,” in *Proceedings of the 18th Americas Conference on Information Systems (AMCIS 2012)*, Seattle, WA, USA.

Sunyaev, A., and Schneider, S. 2013. “Cloud Services Certification,” *Communications of the ACM* (56:2), pp. 33–36.

Tauber, M., Wagner, C., and Pallas, F. 2014. “Sicherheit und rechtliche Herausforderungen in Bezug auf Cloud Computing und Kritische Infrastruktur-IT,” *e & i Elektrotechnik und Informationstechnik* (131:1), pp. 33–36.

Ten, C., and Manimaran, G. 2010. “Cybersecurity for Critical Infrastructures: Attack and Defense Modeling,” *IEEE Transactions on Systems, Man, and Cybernetics – Part A: Systems and Humans* (40:4), pp. 853–865.

Teuteberg, F. 2015. “Kennzahlengestütztes Risikomanagement zum Monitoring von IT-Outsourcing-Aktivitäten am Beispiel des Cloud Computing,” *Controlling – Zeitschrift für erfolgsorientierte Unternehmenssteuerung* (27:6), pp. 290–299.

Venkatesh, V., Brown, S. A., and Bala, H. 2013. “Bridging the Qualitative-Quantitative Divide: Guidelines for Conducting Mixed Methods Research in Information Systems,” *MIS Quarterly* (37:1), pp. 21–54.

VHB. 2015. “Teilrating Wirtschaftsinformatik,” (available at https://www.vhbonline.org/VHB4you/jourqual/vhb-jourqual-3/teilrating-wi/; retrieved October, 31, 2019)

Wagner, C., Hudic, A., Maksuti, S., Tauber, M., and Pallas, F. 2015. “Impact of Critical Infrastructure Requirements on Service Migration Guidelines to the Cloud,” in *Proceedings of the 3rd International Conference on Future Internet of Things and Cloud (FiCloud 2015)*, Rome, Italy.

Walnum, H. J., and Andrae, A. S. G. 2016. “The Internet: Explaining ICT Service Demand in Light of Cloud Computing Technologies,” in *Rethinking Climate and Energy Policies: New Perspectives on the Rebound Phenomenon*, T. Santarius, H. J. Walnum, and C. Aall (eds.), Cham, Switzerland: Springer, pp. 227–241.

Walsham, G. 2006. “Doing Interpretive Research,” *European Journal of Information Systems* (15:3), pp. 320–330.

Walsham, G. 1993. *Interpreting Information Systems in Organizations*, New York, NY, USA: John Wiley & Sons.

Walterbusch, M., Martens, B., and Teuteberg, F. 2013. "Exploring Trust in Cloud Computing: A Multi-Method Approach," in *Proceedings of the 21st European Conference on Information Systems (ECIS 2013)*, Utrecht, Netherlands.

Walterbusch, M., and Teuteberg, F. 2012. "Vertrauen im Cloud Computing," *HMD – Praxis der Wirtschaftsinformatik* (49:6), pp. 50–59.

Webster, J., and Watson, R. T. 2002. "Analyzing the Past to Prepare for the Future: Writing a Literature Review," *MIS Quarterly* (26:2), pp. xiii–xxiii.

Weintraub, E., and Cohen, Y. 2016. "Security Risk Assessment of Cloud Computing Services in a Networked Environment," *International Journal of Advanced Computer Science and Applications* (7:11), pp. 79–90.

Wilde, T. 2008. *Experimentelle Forschung in der Wirtschaftsinformatik*, Hamburg, Germany: Verlag Dr. Kovač.

Wilde, T., and Hess, T. 2007. "Forschungsmethoden der Wirtschaftsinformatik – Eine empirische Untersuchung," *Wirtschaftsinformatik* (49:4), pp. 280–287.

Yin, R. K. 2018. *Case Study Research and Applications: Design and Methods*, Thousand Oaks, CA, USA: Sage.

Younis, Y. A., Merabti, M., and Kifayat, K. 2013. "Secure Cloud Computing for Critical Infrastructure: A Survey," in *Proceedings of the 14th Annual Post Graduate Symposium on The Convergence of Telecommunications, Networking and Broadcasting (PGNet 2013)*, Liverpool, UK.

Yusta, J. M., Correa, G. J., and Lacal-Arántegui, R. 2011. "Methodologies and Applications for Critical Infrastructure Protection: State-of-the-Art," *Energy Policy* (39:10), pp. 6100–6119.

Zissis, D., and Lekkas, D. 2012. "Addressing Cloud Computing Security Issues," *Future Generation Computer Systems* (28:3), pp. 583–592.

# Part B: Research Contributions

**Contribution A**

## Cloud Computing Adoption in Critical Infrastructures – Status Quo and Elements of a Research Agenda

| | |
|---|---|
| Authors | Adelmeyer, M.; Teuteberg, F. |
| Year | 2018 |
| Outlet | Proceedings of the Multikonferenz Wirtschaftsinformatik (MKWI 2018), Lüneburg, Germany |
| Identification | ISBN 978-3-935786-72-0 |
| Online | http://mkwi2018.leuphana.de/programm/tagungsband/ |

# Cloud Computing Adoption in Critical Infrastructures – Status Quo and Elements of a Research Agenda

Michael Adelmeyer, Frank Teuteberg

Universität Osnabrück
Fachgebiet Unternehmensrechnung und Wirtschaftsinformatik,
Osnabrück
{michael.adelmeyer;frank.teuteberg}@uni-osnabrueck.de

**Abstract.** Critical infrastructures, as the backbone of societal life, become increasingly dependent on IT. Thus, in order to ensure security and resilience, they face strict IT legislations and requirements. However, due to efficiency benefits, such as cost savings and increased flexibility, critical infrastructures increasingly adopt innovative IT models like cloud computing. This is despite the fact that migrating processes or systems into a cloud involves major risks for sensitive IT landscapes, since the control over data and security measures is delegated to cloud providers. In order to identify the current status quo of cloud computing in critical infrastructures, we conduct a systematic literature review, an analysis of cloud-based outsourcings of German critical infrastructures and expert interviews. Our findings provide an overview and a research agenda of cloud usage in critical sectors, which are helpful for critical infrastructure and cloud providers alike in order to adopt or manage cloud solutions.

**Keywords.** Cloud Computing, Critical Infrastructures, IT Security, IT Risks

**Contribution B**

### Die Auswirkungen des IT-Sicherheitsgesetzes auf die Interne Revision *(Translation: The Impacts of the IT Security Law on Internal Auditing)*

| | |
|---|---|
| Authors | Goldshteyn, M.; Adelmeyer, M. |
| Year | 2015 |
| Outlet | Zeitschrift Interne Revision (50:6), pp. 244–255 |
| Identification | ISSN 0044-3816 |
| Online | https://www.zirdigital.de/ZIR.06.2015.244 |

# Die Auswirkungen des IT-Sicherheitsgesetzes auf die Interne Revision

Michael Goldshteyn, Michael Adelmeyer

Universität Osnabrück
Fachgebiet Unternehmensrechnung und Wirtschaftsinformatik,
Osnabrück
michael.adelmeyer@uni-osnabrueck.de

**Abstract.** Die Sicherheit und der Schutz von IT-Systemen gewinnen in der heutigen Unternehmenslandschaft zunehmend an Bedeutung. Aus diesem Grund hat der Gesetzgeber das IT-Sicherheitsgesetz verabschiedet. Hierdurch soll eine signifikante Verbesserung der Sicherheit informationstechnischer Systeme herbeigeführt und Kritische Infrastrukturen besser vor Cyberangriffen geschützt werden. Nach einer Darstellung der Änderungen und ihrer kritischen Würdigung wird der Frage nachgegangen, welche Auswirkungen die Gesetzesnovelle auf Unternehmen selbst und die Arbeit der Internen Revision entfaltet. Anschließend werden Handlungsempfehlungen ausgesprochen.

**Contribution C**

## IT-Risikomanagement von Cloud-Services in Kritischen Infrastrukturen *(Translation: IT Risk Management of Cloud Services in Critical Infrastructures)*

| | | |
|---|---|---|
| Authors | Adelmeyer, M., Petrick, C., Teuteberg, F. | |
| Year | 2018 | |
| Outlet | Wiesbaden, Germany: Springer Vieweg | |
| Identification | DOI | 10.1007/978-3-658-22742-5 |
| | eBook ISBN | 978-3-658-22742-5 |
| | Softcover ISBN | 978-3-658-22741-8 |
| Online | https://www.springer.com/de/book/9783658227418 | |

# IT-Risikomanagement von Cloud-Services in Kritischen Infrastrukturen

Michael Adelmeyer, Christopher Petrick, Frank Teuteberg

Universität Osnabrück
Fachgebiet Unternehmensrechnung und Wirtschaftsinformatik,
Osnabrück
{michael.adelmeyer;cpetrick;frank.teuteberg}@uni-osnabrueck.de

**Abstract.** Der Einsatz von Cloud-Services birgt neben vielfältigen Vorteilen auch Risiken für die IT-Sicherheit von Unternehmen. Dies gilt insbesondere für Betreiber Kritischer Infrastrukturen, die durch das IT-Sicherheitsgesetz dazu verpflichtet werden, ihre IT besser vor Cyber-Attacken zu schützen. Für ein funktionierendes IT-Risiko- und Sicherheitsmanagement ist daher eine vollständige Identifikation sowie Bewertung der sich aus dem Einsatz von Cloud-Services ergebenden Risiken unerlässlich. Hierzu werden im vorliegenden essential ein Anforderungskatalog an Cloud-Services zur Umsetzung des IT-Sicherheitsgesetzes, ein Framework für das IT-Risikomanagement von Cloud-Services in Kritischen Infrastrukturen sowie Handlungsempfehlungen für Unternehmen präsentiert.

**Contribution D**

## Trust Transitivity and Trust Propagation in Cloud Computing Ecosystems

| | |
|---|---|
| Authors | Adelmeyer, M.; Walterbusch, M.; Biermanski, P.; Teuteberg, F. |
| Year | 2018 |
| Outlet | Proceedings of the 26th European Conference on Information Systems (ECIS 2018), Portsmouth, UK |
| Online | https://aisel.aisnet.org/ecis2018_rp/29 |

# Trust Transitivity and Trust Propagation in Cloud Computing Ecosystems

Michael Adelmeyer, Marc Walterbusch, Peter Biermanski, Frank Teuteberg

Universität Osnabrück
Fachgebiet Unternehmensrechnung und Wirtschaftsinformatik,
Osnabrück
{michael.adelmeyer;marc.walterbusch;pbiermanski;frank.teuteberg}@uni-osnabrueck.de

**Abstract.** Due to security and privacy concerns, trust is a vital facilitator of successful business relationships in cloud computing ecosystems. This is especially true when customers obtain adapted services built on third-party cloud services. In this case, customers are no longer interacting with service providers directly. Instead, they rely on mediators and, thus, are dependent on the mediators' choices and judgement. Hence, we analyze the role of trust transitivity and propagation – the derivation of a certain amount of trust from a trust relationship with a directly known party – between individual customers and mediators as well as service providers in an online experiment. The results reveal no significant evidence for trust transitivity (complete propagation of the level of trust between the actors) in cloud computing trust chains. Rather, individual customers' trust is propagated between mediators and cloud service providers. This evidence is important for providers, as they could mitigate direct trust issues by providing services indirectly. Further, mediators should be aware that trust and consequently the usage behavior of individual customers can be affected by incidents which are caused by providers. For science, this understanding is vital to further examine and understand the role of trust in cloud adoption and usage.

**Keywords.** Cloud Computing, Trust, Transitivity, Propagation, Usage Intention, Online Experiment

**Contribution E**

## Eye-Tracking zur Untersuchung von Vertrauenssignalen auf Webseiten von Cloud Computing-Anbietern *(Translation: Eye-Tracking for the Investigation of Trust Signals on Websites of Cloud Computing Providers)*

| | | |
|---|---|---|
| Authors | Adelmeyer, M.; Beinke, J. H.; Walterbusch, M.; Gameiro, R. R.; König, P.; Teuteberg, F. | |
| Year | 2016 | |
| Outlet | Proceedings of the 46. Jahrestagung der Gesellschaft für Informatik (INFORMATIK 2016), Lecture Notes in Informatics, Klagenfurt, Austria | |
| Identification | ISBN | 978-3-88579-653-4 |
| | ISSN | 1617-5468 |
| Online | https://dl.gi.de/20.500.12116/1196 | |

# Eye-Tracking zur Untersuchung von Vertrauenssignalen auf Webseiten von Cloud Computing-Anbietern

Michael Adelmeyer[1], Jan Heinrich Beinke[1], Marc Walterbusch[1], Ricardo Ramos Gameiro[2], Peter König[2,3], Frank Teuteberg[1]

[1] Universität Osnabrück
Fachgebiet Unternehmensrechnung und Wirtschaftsinformatik,
Osnabrück
{michael.adelmeyer;jan.beinke;marc.walterbusch;frank.teuteberg}@uni-osnabrueck.de

[2] Universität Osnabrück
Institut für Kognitionswissenschaft,
Osnabrück
{pkoenig;rramosga}@uni-osnabrueck.de

[3] Universitätsklinikum Hamburg-Eppendorf,
Institut für Neurophysiologie und Pathophysiologie,
Hamburg

**Abstract.** Durch die dynamische Bereitstellung von Ressourcen bietet Cloud Computing Unternehmen die Möglichkeit Effizienz- und Wettbewerbsvorteile zu realisieren. Aufgrund der mit der Technologie einhergehenden Delegation der Kontrolle über eigene Daten und Services haben viele Unternehmen jedoch Vorbehalte, insbesondere in Hinblick auf Datensicherheits- und Datenschutzaspekte. Durch Vertrauenssignale, wie Zertifikate, Kundenbewertungen, Referenzkunden und vertrauensrelevante Informationen wie zum Beispiel zur Ausfallsicherheit, können Cloud-Anbieter der Informationsasymmetrie entgegenwirken und Vertrauen erzeugen. Um die Wahrnehmung und den Effekt der Platzierung solcher Vertrauenssignale auf Anbieter-Webseiten zu untersuchen, wurde im vorliegenden Beitrag eine Eye-Tracking Studie durchgeführt. Die Ergebnisse der Untersuchung deuten auf eine Bestätigung der positiven Wahrnehmung sowie den positiven Auswirkungen der Vertrauenssignale hin. Hierbei werden sicherheitsbezogene Signale als positiver vertrauensbeeinflussend wahrgenommen als soziale.

**Keywords.** Cloud Computing, Vertrauen, Eye-Tracking, IT-Sicherheit, Vertrauenssignale

**Contribution F**

## Does the Augmentation of Service Level Agreements Affect User Decisions in Cloud Adoption Scenarios? – An Experimental Approach

| | |
|---|---|
| Authors | Adelmeyer, M.; Seifert, K.; Walterbusch, M.; Teuteberg, F. |
| Year | 2016 |
| Outlet | Proceedings of the 24th European Conference on Information Systems (ECIS 2016), Istanbul, Turkey |
| Online | https://aisel.aisnet.org/ecis2016_rp/95/ |

# Does the Augmentation of Service Level Agreements Affect User Decisions in Cloud Adoption Scenarios? – An Experimental Approach

Michael Adelmeyer, Marc Walterbusch, Kai Seifert, Frank Teuteberg

Universität Osnabrück
Fachgebiet Unternehmensrechnung und Wirtschaftsinformatik,
Osnabrück
{michael.adelmeyer;marc.walterbusch;kaseifert;frank.teuteberg}@uni-osnabrueck.de

**Abstract.** Despite the benefits of cloud computing, customers are reluctant to use cloud services as they have concerns about data security and privacy. Many of these concerns arise due to the lack of transparency. Consequently, bridging the existing information asymmetry and, thus, fostering trust in the cloud provider is of high relevance. As service level agreements are an important trust building factor and due to their technical and complex nature, the augmentation of these is promising. Therefore, we investigate the effects of augmenting service level agreements (by means of augmented browsing) on the ease of the information gathering process and simultaneously on perceived information overload, comprehension and transparency in a web-based experiment. The results of our online experiment do not confirm our assumed positive effects of augmentation. Nonetheless, we show that the ease of gathering information about a cloud service positively influences the perceived trustworthiness. Furthermore, we demonstrate that the perceived trustworthiness of a cloud computing provider largely determines the intention to use its services. Thus, besides improving security, cloud providers not only have to communicate trust-critical information but also have to identify suitable measures of information provisioning that considerably improve transparency while lowering information overload.

**Keywords.** Cloud Computing, Augmentation, Information Overload, Comprehension, Transparency, Trust, Service Level Agreements

**Contribution G**

**Datenanalysen in der Cloud – Konzeption einer Architektur für die Wirtschaftsprüfung** ***(Translation: Data Analyses in the Cloud – Conception of an Architecture for Auditing)***

| | | |
|---|---|---|
| Authors | Adelmeyer, M.; Teuteberg, F. | |
| Year | 2018 | |
| Outlet | Cloud Computing, S. Reinheimer (ed.), Wiesbaden, Germany: Springer Fachmedien, pp. 89–102. | |
| Identification | DOI | 10.1007/978-3-658-20967-4_7 |
| | Online ISBN | 978-3-658-20967-4 |
| | Print ISBN | 978-3-658-20966-7 |
| Online | https://link.springer.com/chapter/10.1007/978-3-658-20967-4_7 | |

# Datenanalysen in der Cloud – Konzeption einer Architektur für die Wirtschaftsprüfung

Michael Adelmeyer, Frank Teuteberg

Universität Osnabrück
Fachgebiet Unternehmensrechnung und Wirtschaftsinformatik,
Osnabrück
{michael.adelmeyer;frank.teuteberg}@uni-osnabrueck.de

**Abstract.** Die Digitalisierung von Prozessen in Unternehmen führt zu einem rasanten Anstieg der Datenmengen. Um die Datenflut zu beherrschen, muss die Wirtschaftsprüfung neue Methoden und IT-Architekturen entwickeln und integrieren. Der Einsatz von Cloud Computing für rechen- und speicherintensive Datenanalysen verspricht im Vergleich zu klassischen IT-Architekturen die Realisierung von Effizienzpotenzialen und die Ermöglichung neuartiger Prüfungsansätze. Jedoch müssen Cloud-spezifische Risiken und Anforderungen berücksichtigt werden, zum Beispiel in Bezug auf den Schutz und die Sicherheit von teils sensiblen Mandantendaten sowie deren rechtskonforme Speicherung und Verarbeitung. Der vorliegende Beitrag basiert auf einer Erhebung in einer führenden Wirtschaftsprüfungsgesellschaft, die im Vorfeld zur Einführung einer Cloud-Architektur durchgeführt wurde. Es werden Herausforderungen und Potenziale aufgezeigt sowie eine Cloud-Architektur für Datenanalysen in der Wirtschaftsprüfung vorgestellt.

**Keywords.** Cloud-Architektur, Wirtschaftsprüfung, Datenanalysen, Private Cloud, IT-Sicherheit, Digitalisierung

**Contribution H**

## RisCC – A Risk Management Tool for Cloud Computing Environments

| | | |
|---|---|---|
| Authors | Adelmeyer, M.; Beike, L.; Buggenthin, M.; Osada, S.; Teuteberg, F. | |
| Year | 2018 | |
| Outlet | Proceedings of the 24th Americas Conference on Information Systems (AMCIS 2018), New Orleans, LA, USA | |
| Identification | ISBN | 978-0-9966831-6-6 |
| Online | https://aisel.aisnet.org/amcis2018/Security/Presentations/11/ | |

# RisCC – A Risk Management Tool for Cloud Computing Environments

Michael Adelmeyer, Lukas Beike, Mirko Buggenthin, Sebastian Osada, Frank Teuteberg

Universität Osnabrück
Fachgebiet Unternehmensrechnung und Wirtschaftsinformatik,
Osnabrück
{michael.adelmeyer;lbeike;mbuggenthin;sosada;frank.teuteberg}@uni-osnabrueck.de

**Abstract.** The risks associated with the adoption of cloud computing solutions are dependent on a multitude of factors and vary considerably depending on the selected cloud service and deployment models. In addition, regulatory amendments regarding IT security and privacy trigger the need for flexible risk management solutions for cloud environments in order to adequately identify and manage the associated risks. Thus, the aim of this study is to design and implement a risk management tool for cloud services. By designing a modular and extensible tool, the individual risk profiles of the diverse cloud deployments can be addressed. The tool was developed and evaluated iteratively and by applying multiple methods, including a systematic literature analysis, expert interviews as well as surveys for evaluation. The developed risk management tool is useful for science and practice alike as it enables to effectively address risks resulting from cloud deployments and to adequately incorporate regulatory requirements.

**Keywords.** Cloud Computing, Risk Management, IT Security, Web Application

**Contribution I**

### Datenschutz und Datensicherheit im Cloud Computing – Ein Framework zur Beurteilung von Cloud-Services *(Translation: Data Privacy and Data Security in Cloud Computing – A Framework for the Evaluation of Cloud Services)*

| | | |
|---|---|---|
| Authors | Adelmeyer, M.; Walterbusch, M.; Lang, J.; Teuteberg, F. | |
| Year | 2017 | |
| Outlet | Die Wirtschaftsprüfung (WPg) (70:1), pp. 35-42 | |
| Identification | ISSN | 0340-9031 |

# Datenschutz und Datensicherheit im Cloud Computing – Ein Framework zur Beurteilung von Cloud-Services

Michael Adelmeyer, Marc Walterbusch, Julian Lang, Frank Teuteberg

Universität Osnabrück
Fachgebiet Unternehmensrechnung und Wirtschaftsinformatik,
Osnabrück
{michael.adelmeyer;marc.walterbusch;jlang;frank.teuteberg}@uni-osnabrueck.de

**Abstract.** Unternehmen können durch den Einsatz von Cloud Computing Effizienz- bzw. Wettbewerbsvorteile realisieren. Das Vertrauen der Praxis in diese Technologie ist jedoch nicht uneingeschränkt, vor allem im Hinblick auf Datenschutz und Datensicherheit gibt es Vorbehalte. Durch Audits und damit einhergehende Zertifizierungen kann die Einhaltung grundlegender und definierter Standards bescheinigt werden; allerdings sind die Anforderungen an einen Cloud-Service spezifisch, und der Markt bestehender Standards und Zertifikate für Cloud-Services ist heterogen. Dies stellt den Wirtschaftsprüfer vor die Herausforderung, Datensicherheit und Datenschutz in der Cloud und die daraus entstehenden Risiken angemessen zu beurteilen. Zu diesem Zweck wird ein allgemeines Framework vorgestellt.

**Keywords.** Cloud Computing, Datenschutz, Datensicherheit, Zertifizierung, IT-Audit

**Contribution J**

## Security and Privacy of Personal Health Records in Cloud Computing Environments – An Experimental Exploration of the Impact of Storage Solutions and Data Breaches

| | |
|---|---|
| Authors | Adelmeyer, M.; Meier, P.; Teuteberg, F. |
| Year | 2019 |
| Outlet | Proceedings of the 14th International Conference on Wirtschaftsinformatik (WI 2019), Siegen, Germany |
| Online | https://aisel.aisnet.org/wi2019/track08/papers/1/ |

# Security and Privacy of Personal Health Records in Cloud Computing Environments – An Experimental Exploration of the Impact of Storage Solutions and Data Breaches

Michael Adelmeyer, Pascal Meier, Frank Teuteberg

Universität Osnabrück
Fachgebiet Unternehmensrechnung und Wirtschaftsinformatik,
Osnabrück
{michael.adelmeyer;pascal.meier;frank.teuteberg}@uni-osnabrueck.de

**Abstract.** In the course of the digitization in healthcare, the collection and central storage of large health-related datasets in clouds in the form of personal health records is growing. However, the use of cloud services for sensitive data is associated with security and privacy risks. Further, the delegation of control over security and privacy measures to the cloud provider requires trust on the users' side. In order to investigate the role of security and privacy when storing and processing patient data, we conducted an online experiment, in which third-party cloud services are compared to private on-premise data centers. Additionally, we examine the impact of data breaches on the perceived security, privacy, control and trust in both storage scenarios. Our results indicate that cloud-based personal health records still face concerns regarding perceived security, privacy, control and trust amongst end-users. Nevertheless, after a data breach, no significant differences between both solutions exist.

**Keywords.** Cloud Computing, Personal Health Records, Security, Privacy

**Contribution K**

## Rebound Effects in Cloud Computing: Towards a Conceptual Framework

| | |
|---|---|
| Authors | Adelmeyer, M.; Walterbusch, M.; Biermanski, P.; Seifert, K.; Teuteberg, F. |
| Year | 2017 |
| Outlet | Proceedings of the 13th International Conference on Wirtschaftsinformatik (WI 2017), St. Gallen, Switzerland |
| Online | https://aisel.aisnet.org/wi2017/track05/paper/4/ |

# Rebound Effects in Cloud Computing: Towards a Conceptual Framework

Michael Adelmeyer, Marc Walterbusch, Peter Biermanski, Kai Seifert,
Frank Teuteberg

Universität Osnabrück
Fachgebiet Unternehmensrechnung und Wirtschaftsinformatik,
Osnabrück
{michael.adelmeyer;marc.walterbusch;pbiermanski;kaseifert;frank.teuteberg}@uni-osnabrueck.de

**Abstract.** Rebound effects have been discussed in various disciplines. In the information and communication technology sector, this topic is still insufficiently studied. Basically, a rebound effect is a feedback mechanism, as a result of which savings from efficiency improvements are not or only partially realized. Due to the potential of cloud computing for efficiency improvements, not only in terms of energy efficiency, but also in terms of organizational resources in general, we describe rebound effects in this context by means of a systematic literature review and a case study. Our results provide a framework to categorize and identify potential rebound effects in cloud computing. The understanding of rebound effects and their influence on the various organizational resources (e.g., server hardware, human resources or IT know-how), is important for managers to sustainably decide for or against the adoption, integration and roll out of cloud computing services.

**Keywords.** Rebound Effects, Cloud Computing, Literature Analysis, Case Study, Conceptual Framework