Technische Universität München

Fakultät für Informatik
Lehrstuhl für Wirtschaftsinformatik
Univ.-Prof. Dr. Helmut Krcmar

The Influence of Control Mechanisms on Cloud Sourcing Decisions

Michael Bernhard Lang, Master of Science with honors

Vollständiger Abdruck der von der Fakultät für Informatik der Technischen Universität München zur Erlangung des akademischen Grades eines

Doktors der Naturwissenschaften
(Dr. rer. nat.)

genehmigten Dissertation.

Vorsitzender:	Prof. Dr. Jens Grossklags	
Prüfer der Dissertation:	1.	Prof. Dr. Helmut Krcmar
	2.	Prof. Dr. Martin Bichler

Die Dissertation wurde am 02.10.2018 bei der Technischen Universität München eingereicht und durch die Fakultät für Informatik am 26.02.2019 angenommen.

Preface

Am I going to write my Masters' Thesis in Munich or in Augsburg? After a discussion with Michael Schermann and Stefan Hörmann I knew the answer – let's do some research at the Chair for Information Systems at TUM. After getting addicted to quantitative research methods, I decided to apply for a Ph.D. position and broaden my horizon within the challenging but also supportive environment at the same chair. Today, more than four years later, I do not regret this decision. I am glad to have taken this journey, which allow me to grow into a more confident, resilient, and knowledgeable designer.

The most important mentor and Ph.D. advisor throughout all years was Professor Helmut Krcmar. Both, on a professional and personal level, he inspired and motivated me continuously. While I received the freedom to select the focus of my dissertation project, at the same time Professor Krcmar assured that the chosen direction would be successful by always asking the right questions. I thank him and the entire chair for giving me the opportunity to participate and grow during projects like the establishment of the "Initiative for Digital Transformation" and the Design Thinking program at TUM derived from the global SUGAR-network.

Also such a journey would not have been possible without the support of my research group leader Manuel Wiesche and my dear colleagues. Manuel encouraged and motivated me to continuously focus on my research topics. Through the sometimes strenuous but always fruitful discussions, Manuel shaped many of the publications embedded in this thesis. Moreover, having good colleagues and friends within my dissertation process to exchange, get inspired and motivated was also very helpful for me. A big thank goes to Christoph Pflügler, Tobias Riasanow, Maximilian Schreieck, and Harald Kienegger, whose acute sense of humor made my Ph.D. experience a very enjoyable one.

Last, my biggest gratitude goes to my dear parents, Bernhard and Sabine Lang, my brother Philipp Lang, and my friends from the A-Team. My parents tremendously supported me throughout my entire life. My friends, including my brother, are responsible for many joyous and memorable moments, not only in the last four years. My family and friendships are the most valuable assets I have.

Munich, September 2018 Michael Lang

Abstract

Problem Statement: Despite the growing body of knowledge and the crucial impact on competitive advantages for cloud customers, organizations have still a low and different adoption rate of cloud services across countries. This thesis addresses four major challenges in the field of information technology outsourcing in general, and particular of cloud sourcing that are not addressed in extant research: (1) missing focus on micro-level as unit of analysis, (2) fragmented research on control mechanisms, (3) missing integration of psychological control perspective, and (4) assurance seals are handled as a black box. By investigating decision making in cloud sourcing projects on a micro level, this thesis contributes to a more nuanced understanding of the cognitive decision-making process as the basis for the success of information technology outsourcing and cloud adoption.

Research Design: Following the pragmatic paradigm and a mixed strategy of inquiry, this thesis employs both, qualitative and quantitative research methods to address the mentioned challenges and the derived research questions.

Results: The results of this thesis comprise a characterization of control mechanisms in an online environment, identification of similarities and differences between information technology outsourcing and cloud sourcing, empirical ranking and longitudinal analysis of Quality-of-Service attributes from customers' perspective, classification and testing of the influence of three control agents – namely personal control, proxy control, and collective control – on cloud customers' perceived privacy in two cultures, and identification of certification authorities' reputation and the quality level of an audit as determinants of the effectiveness of assurance seals in a professional cloud environment.

Contribution: In general, this thesis contributes to theory and practice by addressing the four challenges mentioned above, e.g., by (1) focusing on a micro-level as unit of analysis, by (2) providing and testing a conceptualization of research on control mechanisms, by (3) integrating the rich body of psychologic control literature in cloud sourcing research, and by (4) investigating what determines the effectiveness of assurance seals. The contribution to theory relates to an improved understanding of variables, relationships, reasoning, and boundary conditions relating to cloud sourcing projects. The contribution to practice comprises a set of guidelines for (potential) cloud customers, cloud service providers, and certification authorities.

Study Limitations: This thesis is subject to several limitations. First of all, although this thesis gives a relatively broad overview of cloud sourcing research, it focuses on cloud sourcing projects in a professional environment and, in particular, on decision makers' perceived privacy. Hence, generalizability of the findings may be limited. Additionally, some empirical analyses are based on non-experimental data. Hence, the findings of this thesis are potentially exposed to internal validity threats. Furthermore, each empirical analysis included in this thesis is subject to specific validity threats such as construct validity or statistical conclusion validity.

Future Research: Based on its findings and limitations, this thesis identifies several avenues for future research. These include the identification of a trade-off between cloud and edge computing, the comparison of professional and end-consumer cloud selection decisions, the privacy impact on individual, organizational, and national level, an interplay between cloud computing and supra-national regulations and policy frameworks, and the impact of security breaches and hacker attacks on decision makers’ preferences for control mechanisms.

Table of Contents

List of Figures

List of Tables

List of Appendices

List of Abbreviations

A	Assumption
C	Challenge
CC	Cloud Computing
CIO	Chief Information Officer
CSP	Cloud Service Provider
CON	Conference
CRM	Customer Relationship Management
ECIS	European Conference on Information Systems
EJIS	European Journal of Information Systems
GDPR	General Data Protection Regulation
HICSS	Hawaii International Conference on System Sciences
IaaS	Infrastructure-as-a-Service
I&M	Information & Management
IS	Information Systems
IT	Information Technology
ITO	Information Technology Outsourcing
JNL	Journal
M	Method
O	Outcome
P	Publication
PaaS	Platform-as-a-Service
QoS	Quality-of-Service
RQ	Research Question
SaaS	Software-as-a-Service
VHB	Verband der Hochschullehrer für Betriebswirtschaft
WI	International Conference on Wirtschaftsinformatik

Part A

1 Introduction

1.1 Problem Statement

The worldwide spending on cloud computing (CC) grew by 18.5% to $260 billion between 2016 and 2017 (Nag 2017). Gartner predicts a five-year growth rate of 16.9% through 2021 in cloud services with infrastructure-as-a-service (IaaS) leading the segment at 30.2% in 2017 (Nag 2017). To benefit from this development, a growing number of cloud service providers (CSPs) have entered the CC market by providing distinct cloud services (Kourtesis et al. 2014; Menzel et al. 2015). Prominent examples are Amazon, Google, Microsoft, Rackspace, and GoGrid, who are providers of IaaS and platform-as-a-service (PaaS). SalesForce, Cisco WebEx and DATEV are well-known providers of software-as-a-service (SaaS).

From the cloud customers' point of view, however, when using cloud services, they pool their resources outside of the firm's environment and increase their dependency on third parties and networks (Brender/Markov 2013). As a consequence, cloud customers face risks like poaching resulting from malicious behavior in shared environments (Clemons/Hitt 2004) or the risk of service breakdowns, because of possible network outages (Subashini/Kavitha 2011). At the same time, an increasing number of laws, policies, and rules forces cloud customers to consider additional requirements such as data protection (Ragowsky et al. 2014; Schneider/Sunyaev 2016). To identify the right CSP, cloud customers have only a few means like assurance seals or privacy policies, even if high uncertainty during decision making exist (Schneider/Sunyaev 2016). Therefore, cloud customers struggle to identify suitable CSPs and, in the worst case, do not adopt cloud services.

To address these challenges research investigated cloud sourcing decisions on two different levels (Schneider/Sunyaev 2016): macro and micro level. Research on a macro level investigates how technology, organizational, or environmental factors influence companies whether to use CC or not (Low et al. 2011). As an example, a company's need for technology customization, access to specialized resources, the company size, or internal cost pressure facilitate cloud sourcing (Gupta et al. 2013; Brender/Markov 2013). Contrary, legal and security concerns, low level of standardization, or social factors inhibit cloud sourcing (Lee et al. 2013b; Lin/Chen 2012). Table 1 summarizes the extant literature about cloud sourcing research on a macro level.

Moreover, cloud sourcing practices involve major management decisions. In this respect, research examined cloud sourcing on a micro level and investigates how CIO skills or top management support facilitate the cloud adoption (Blaskovich/Mintchik 2011; Lian et al. 2014). Further, subjective norms influence decision makers during the cloud sourcing decision process (Benlian 2009). Benlian/Hess (2011) note, it is important to understand the associated (cognitive) processes influencing the behavior of cloud customers. Therefore, Benlian/Hess (2011) investigated the sourcing opportunities of cloud sourcing and the risks decision makers face. They concluded that cloud customers are more likely to increase cloud adoption, if they can reduce any perceived privacy risks through appropriate control over sensitive information. Table 2 summarize the extant literature about cloud sourcing research at the micro level.

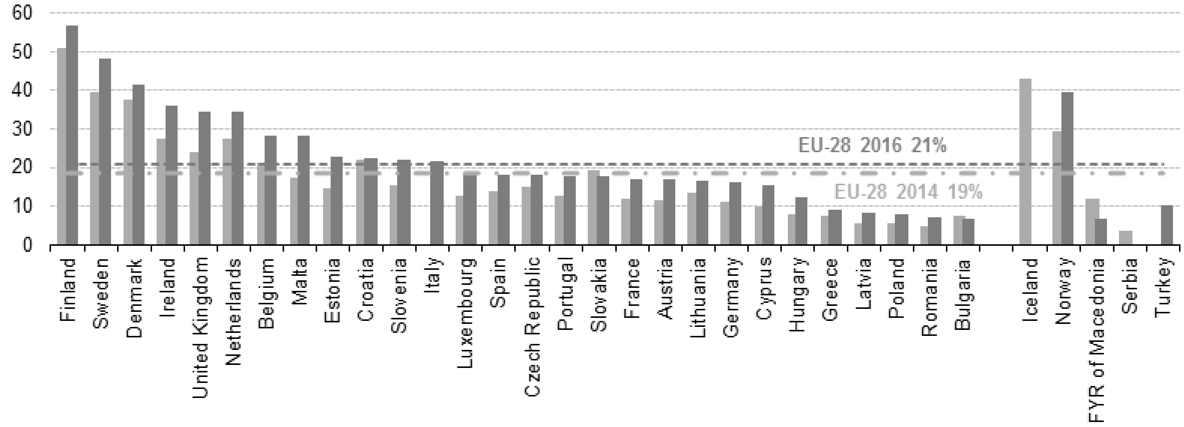
Source	Focus	Research approach	Level of analysis	Selection criteria
Brender/Markov (2013)	Cloud	Qualitative	Macro/firm level	Company size, risk awareness
Gupta et al. (2013)	Cloud	Quantitative	Macro/firm level	Cost reduction, ease of use and convenience, reliability, sharing and collaboration, security and privacy advantages
Heart (2010)	SaaS	Quantitative	Macro/firm level	Reputation of provider, perceived risks, perceived capabilities
Lee et al. (2013b)	SaaS	Qualitative	Macro/firm level	Customization and economic as drivers; social and political factors as inhibitors
Lin/Chen (2012)	Cloud	Qualitative	Macro/firm level	Legal concerns, IS development concerns, security concerns, product uncertainties
Low et al. (2011)	Cloud	Quantitative	Macro/firm level	Technology (Relative advantage, complexity, compatibility); Organization (Top management support, Firm size, Technology readiness); Environment (Competitive pressure, Trading partner pressure)
Wu et al. (2011)	SaaS	Qualitative	Macro/firm level	Strategic-oriented benefits, economic-oriented benefits, subjective risks, technical risks.

Table 1. Cloud sourcing research on a macro level (adopted from Schneider/Sunyaev (2016))

Source	Focus	Research approach	Level of analysis	Selection criteria
Benlian et al. (2009)	SaaS	Quantitative	Micro/Macro	Subjective norms, strategic value, application inimitability, application specificity, application adoption uncertainty
Benlian/Hess (2011)	SaaS	Quantitative	Micro/Macro	Cloud risks (Performance, economic, strategic, security, managerial); Cloud advantages (costs, strategic, focus on core-competencies, resources, quality)
Blaskovich/Mintchik (2011)	SaaS	Quantitative	Micro/individual level	CIO skills
Lian et al. (2014)	Cloud	Quantitative	Micro/Macro	Data security, perceived technical competence, cost, top manager support, and complexity

Table 2. Cloud sourcing research on a micro level (adopted from Schneider/Sunyaev (2016))

Selecting the “right” CSP is essential to assure future performance and maintain compliance with laws, policies, and rules (Garrison et al. 2012; Garrison et al. 2015; Weinhardt et al. 2009; Ragowsky et al. 2014). Therefore, despite the growing body of knowledge and the crucial impact on competitive advantages for cloud customers, companies still are concerned regarding the adoption of CC (Giannakouris/Smihily 2016). Eurostat, the statistical office of the European Union, reports on the adoption of CC an average adoption rate of 19% in 2014 and 21% in 2016 (Figure 1). However, significant differences can be observed across countries. In Finland, Sweden and Denmark, over 40 % of enterprises used CC. On the other hand, fewer than 10 % did so in Greece, Latvia, Poland, Romania and Bulgaria (Giannakouris/Smihily 2016). As a consequence, many companies in different countries avoid cloud sourcing and neglect possible competitive advantages (Mell/Grance 2011).



Italy: break in series; Iceland, Serbia: 2016 not available; Turkey: 2014 not available

Figure 1. Use of cloud computing services in enterprises, 2014 and 2016 (% of enterprises) (Adopted from Giannakouris/Smihily (2016))

In sum, industry reports and academic studies both still point out that adopting new technologies, such as CC, is a complex phenomenon. As a consequence, (potential) cloud customers of different countries demand for decision support during cloud sourcing decisions (Schneider/Sunyaev 2016). With these high non-cloud adoption rate in mind, we argue that the understanding of CSP selection is limited. We identify four fundamental challenges (C) that have not been addressed in extant IS research:

> **C1: Missing focus on micro level as unit of analysis.** Previous studies examining cloud souring decisions are mainly drawn on different economic and organizational theories to explain why firms decide to cloud source or refrain from it (Schneider/Sunyaev 2016). These theories include diffusion of innovation theory (Karunagaran et al. 2016; Kung/Kung Dr 2013), the technology-organization environment framework (Karunagaran et al. 2016), institutional theory (Kung/Kung Dr 2013), resource based view (Messerschmidt/Hinz 2013), or real option theory (Saya et al. 2010). These theories have mainly contributed to our understanding of cloud sourcing outcomes. However, only a few research studies drawing on these theories have focused on the decision-making process itself (e.g., Benlian/Hess (2011)) and, thus, on how cloud customers arrive at cloud sourcing decisions by having extensive judgment about how to control their sensitive information within a cloud environment.

Owing to their main emphasis on the organizational level of analysis, economic and organizational theories have rarely addressed the (cognitive) process that influences individuals' behavior (e.g., key decision-makers in firms). These theories have therefore treated decision-making as a "black box". However, since the adoption of cloud sourcing practices is a major management decision made by individuals rather than organizations, further research is necessary on a micro level (Benlian/Hess 2011; Schneider/Sunyaev 2016).

C2: Fragmented research on control mechanisms. To gain knowledge of the incentive structure surrounding a (potential) relationship, individuals seek control mechanism that provide additional information about (potential) partners (Williams 1997). These control mechanism either accumulate information sufficient for allowing to be certain about (potential) partner's intentions, provide deterrence against unilateral defection, or induce the partner to take a certain course of action with the use of strategies such as "tit-for-tat" (Yamagishi/Yamagishi 1994; Axelrod/Hamilton 1981; Shapiro et al. 1992). Control mechanisms are identified as import antecedents to form users' perceptions, e.g., privacy perceptions, in an online environment (Pavlou 2002; Xu et al. 2012b; Kim 2008). However, a coherent and interrelated structure of these control mechanisms is missing, and the literature would benefit from a conceptualization of these control mechanisms.

C3: Missing integration of psychological control perspective. Research on control mechanisms, which considers the knowledge about the incentive structure surrounding (potential) relationships, can apply a control agency perspective. In particular, this perspective allows not only an examination of the effects of personal control in which the individual acts as an assurance agent to protect information, but also includes proxy control and collective control (Xu et al. 2012b; Yamaguchi 2001). In proxy control, powerful others (such as the government and certification authorities) act as the assurance agents (Xu et al. 2012b; Yamaguchi 2001). In collective control, a collective acts as the assurance agent (Yamaguchi 2001). However, theorists have not integrated the rich literature on psychological control into their theories of individuals' behavior. Consequently, the understanding of perceived assurance as psychological control has not contributed as much as it should have to clarify decision makers' CSP selection behavior (Margulis 2003; Bélanger/Crossler 2011; Skinner 1996).

C4: Assurance seals are handled as a black box. Despite the popularity of assurance seals and a number of studies investigating their effectiveness, no consensus has been reached regarding their impact on online transaction outcomes: Some studies document a positive relationship between third-party certification and purchasing of products (Oezpolat et al. 2013), developing trust in online vendor (Hu et al. 2010) and in ISO9000 certified manufacturing programs (Terlaak/King 2006). Yet, others (e.g., Keith et al. (2015)) find that third-party certification does not necessarily improve outcomes for consumers. The existing initial research sought explanation by identifying contextual or perceptual contingency factors (Lowry et al. 2012; Gao et al. 2010). The role of certifications and their features in such settings, however, have not yet been explored, although some scholars have conjectured that differences between certifications affect decision makers' behaviours upon certifications (Oezpolat et al. 2013).

1.2 Research Questions

The overall objective of this thesis is to advance the understanding of control mechanisms within the cloud market by tackling selected research gaps in the discipline of information technology outsourcing (ITO) that follow from the above mentioned challenges. Following, we briefly illustrate the research questions (RQ) that will be addressed in this thesis:

The identification of relevant control mechanisms is crucial during CSP selection. In order to provide a first step, a literature review within the CC domain but also related domains like e-commerce provides an overview about which control mechanisms are used.

> ***RQ1:*** *What mechanisms of control are exemplary discussed in information systems literature?*

Research has mentioned a variety of control mechanisms. To better understand, how control mechanisms influence decision makers during cloud sourcing decisions, a conceptualization might lead to further insights.

> ***RQ2:*** *Which concepts are relevant when investigating control mechanisms and how are these concepts related?*

Research identified that cloud sourcing is a specific form of ITO and cloud sourcing can leverage insights from the body of knowledge from ITO literature. While extensive literature exists on the selection criteria for ITO, it remains unclear if those selection criteria hold true for cloud sourcing. Hence, identifying the most important selection criteria helps to better understand the similarities and differences between ITO and cloud sourcing.

> ***RQ3:*** *What are the most important criteria, as identified by experts, for the selection of cloud service providers?*

The cloud market is highly dynamic one, in which legal and technical changes occur constantly. As a consequence, existing research from 2011 and 2013 on the most important Quality-of-Service (QoS) attributes show inconsistencies in terms of the prioritization. In order to better understand how the most important QoS change over time, a comparison might provide general guidance for decision makers.

> ***RQ4:*** *How do the most important QoS attributes change over time by considering environmental changes within the cloud market?*

As decision makers have selected certain CSPs, further details have to be investigated. In particular, data privacy aspects are important since companies transfer confidential information to the CSP. To judge and assure data privacy, decision makers can use different control mechanisms provided from different control agents. However, it remains unclear which control agents influence decision makers privacy perceptions.

> ***RQ5:*** *What kind of control agents do cloud customers consider capable of protecting the privacy of their sensitive information?*

Risk-taking theory suggests that risk perception of clients' decision makers affects their risk mitigation behavior and, therefore, the deployment and selection of control mechanisms. Risk perceptions are influenced by the cultural factor uncertainty avoidance. Therefore, we predict that uncertainty avoidance differs among decision makers and affects what control mechanisms decision makers prefer within cloud sourcing projects.

> ***RQ6:*** *How do cultural differences influence the preference of decision makers regarding their choice of control mechanisms within cloud sourcing projects?*

One commonly used source to control CSP are assurance seals. Such assurance seals promote, that a CSP fulfills certain criteria as required from a respective certification standard. However, assurance seals are handled as a black-box and it remains unknown, which information determine their effectiveness to influence decision makers' privacy perceptions.

> ***RQ7:*** *Which information determine the effectiveness of cloud assurance seals to form customers' privacy perceptions?*

These research questions and the according publications address the challenges mentioned above as illustrated in Table 3.

Challenge not addressed in extant IS research	**RQ1**	**RQ2**	**RQ3**	**RQ4**	**RQ5**	**RQ6**	**RQ7**
C1. Missing focus on micro-level as unit of analysis		●	●	●	●	●	●
C2. Fragmented research on control mechanisms	●	●	●	●	●	●	
C3. Missing integration of psychological control perspective	●				●	●	
C4. Assurance seals are handled as a black box	●				●	●	●

C: challenge; RQ: research question; ●: addresses challenge.

Table 3. Research Questions and Challenges Addressed

1.3 Structure

This cumulative thesis consists of three parts. Part A gives an overview on the thesis by introducing the problem statement, providing an overview on the research objective, and structure of the dissertation (Chapter A1). It introduces the basic terms in the area of control mechanisms in cloud sourcing (Chapter A2) and finally describes the research methods and strategy (Chapter A3). Part B of this thesis consist of six peer-reviewed publications (Chapters B1 to B6). While the first three publications focus on cloud decision in general, the last three publications investigate determinants to influence decision makers' privacy perceptions. Part C concludes this thesis. It consists of four chapters. In chapter C1, the results of the six publications are summarized. Chapter C2 discusses the contributions to research and practice. Chapter C3 outlines the study limitations. Finally, chapter C4 illustrates several anchor points for future research. Figure 2 gives an overview on the structure of this thesis.

In the following paragraphs, we summarize the six publications embedded in part B and illustrated in Table 4. In doing so, the research problem, the methodological approach, and the main contributions of each publication (P) are briefly outlined.

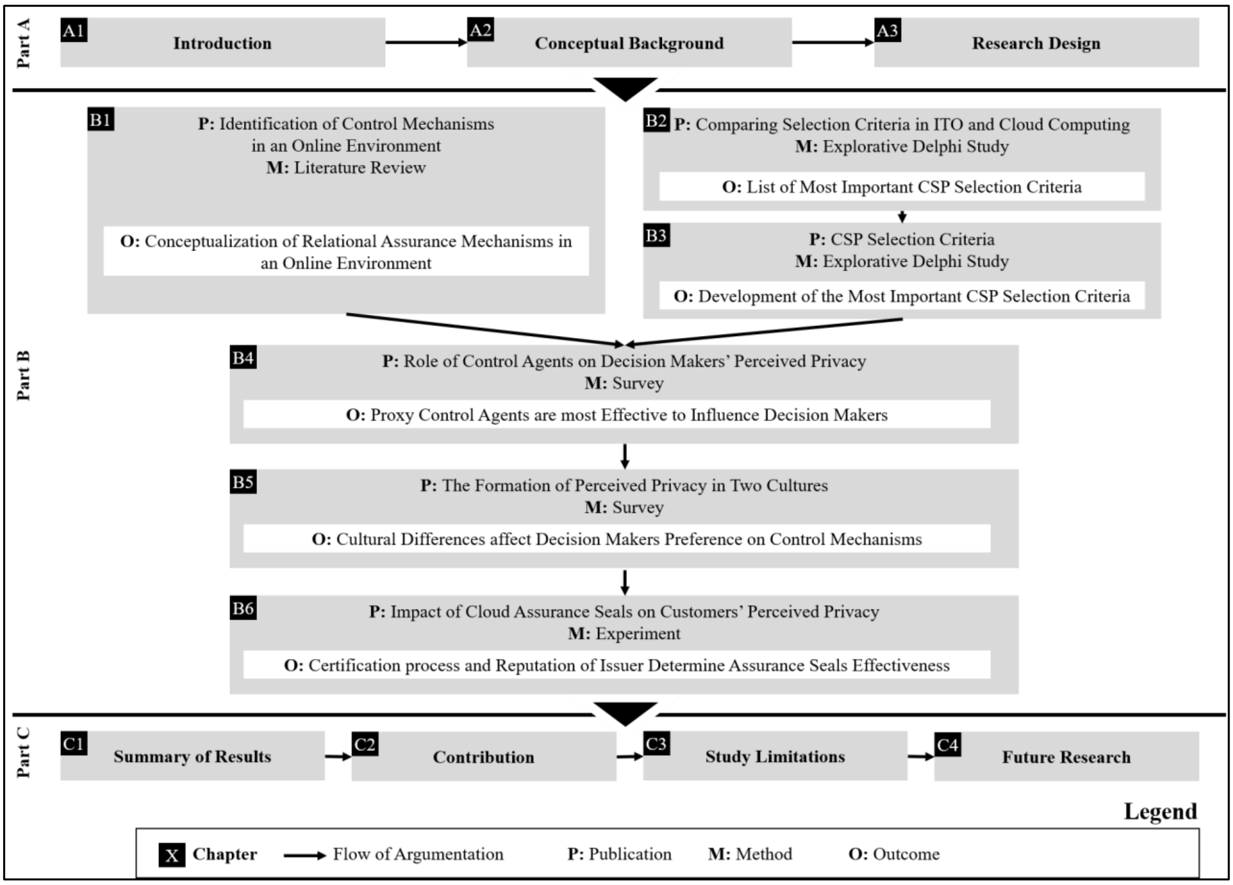

Part A
A1 Introduction
A2 Conceptual Background
A3 Research Design
Part B
B1 P: Identification of Control Mechanisms in an Online Environment
M: Literature Review
O: Conceptualization of Relational Assurance Mechanisms in an Online Environment
B2 P: Comparing Selection Criteria in ITO and Cloud Computing
M: Explorative Delphi Study
O: List of Most Important CSP Selection Criteria
B3 P: CSP Selection Criteria
M: Explorative Delphi Study
O: Development of the Most Important CSP Selection Criteria
B4 P: Role of Control Agents on Decision Makers' Perceived Privacy
M: Survey
O: Proxy Control Agents are most Effective to Influence Decision Makers
B5 P: The Formation of Perceived Privacy in Two Cultures
M: Survey
O: Cultural Differences affect Decision Makers Preference on Control Mechanisms
B6 P: Impact of Cloud Assurance Seals on Customers' Perceived Privacy
M: Experiment
O: Certification process and Reputation of Issuer Determine Assurance Seals Effectiveness
Part C
C1 Summary of Results
C2 Contribution
C3 Study Limitations
C4 Future Research
Legend
X Chapter
Flow of Argumentation
P: Publication
M: Method
O: Outcome

Figure 2. Thesis Structure

P1: Identification of Control Mechanisms in an Online Environment. Control mechanisms are an important element of relational governance and frequently used in information systems (IS) research; still missing in this field, however, is a coherent and interrelated structure to organize available knowledge. In this study, we provide a first step towards development of a conceptualization framework of control mechanisms to enable their further investigation. From our analysis of existing literature, we discover two gaps in assurance research: (1) a fragmentation of control research and (2) a lack of conceptual consensus on control mechanisms. We provide a theoretical framework consisting of a conceptualization of identified control mechanisms, their antecedents and effects as a means of advancing theory in this area. Several possibilities for future research are discussed.

P2: Comparing Selection Criteria in ITO and Cloud Computing. Selecting an appropriate CSP is one of the most important challenges affecting sourcing performance. Although CC relies on the principle of ITO, it remains unclear if selection criteria for ITO providers hold true. Hence, the purpose of this research is to identify the most important criteria for the selection of CSPs. We do this by conducting a Delphi study which includes 16 cloud service decision makers across different cloud service models, company sizes, and industry types. Our results show consensus on CSP selection criteria and identify functionality, legal compliance, contract, geolocation of servers, and flexibility as top five CSP selection criteria. From a theoretical perspective, we demonstrate that results from ITO research hold true for CC research as differences in delivery model and arrangement between ITO and CC will be considered. Practitioners like CSPs and cloud decision makers get guidance from our findings to conduct optimal cloud service investments. This is the first study which provides a comprehensive view on relevant criteria for CSP selection.

P3: CSP Selection Criteria. Customers of CSPs use different criteria to judge the quality of cloud services. Based on managerial and technical QoS attributes, these criteria provide information on service quality and the CSP itself. Thus, it is important to identify relevant QoS to assure success of cloud customers. Using a Delphi study, 16 professionals, who are characterized by different cloud service models, company sizes, and industries, identified and ranked QoS according to their relative importance. Our results show consensus on QoS. We identify functionality, legal compliance, contract, geolocation of servers, and flexibility as top QoS and observe increasing importance of managerial QoS.

P4: Role of Control Agents on Decision Makers' Perceived Privacy. Cloud customers need to assess whether their CSP offers high-quality services and handles sensitive information confidentially. Privacy protection is therefore a major challenge during cloud sourcing. Although cloud customers want control over their sensitive information, they have limited resources to do so. They therefore consider other control agents, such as certification authorities or collectives, but the effectiveness of these groups to ensure privacy protection is unknown. This study differentiates between three control agents (personal control, proxy control, and collective control) and investigates the influence of these agents on cloud customers' perceived control over sensitive information to protect privacy during cloud sourcing. Results show that proxy and collective control influence cloud customers' perceptions, but personal control does not. Therefore, only external control agents, who can apply sanctions, are perceived as being able to effectively protect privacy.

P5: The Formation of Perceived Privacy in Two Cultures. Concerns about privacy risks often inhibit cloud adoption in cloud sourcing projects. To mitigate privacy risks, decision makers use different control mechanisms; namely, direct control, institutional control, and the power of the marketplace. However, cultural context, such as a client's tendency to avoid uncertainty, affects exposure to risks and the selection of control mechanisms. We find cultural differences in the mechanisms used to manage risks when choosing a CSP. Clients from low uncertainty avoidance cultures rely more on their own competence to form privacy perceptions. By contrast, clients from high uncertainty avoidance cultures tend to rely more on the power of the marketplace to form their privacy perceptions. Surprisingly, institutional controls affect decision makers' perceived privacy across all cultures. This is the first study to investigate the cross-cultural formation of perceived privacy during the selection of cloud service provider in cloud sourcing projects.

P6: Impact of Cloud Assurance Seals on Customers' Perceived Privacy. Privacy concerns inhabit professional cloud adoption. Assurance seals resulting from a third-party certification are frequently used from CSPs to provide privacy assurance for their customers. However, empirical findings on the effectiveness of assurance seals focusing on "who" issues those, even if cloud customers also require the information why the assurance seal is valid and reliable. To fill this gap, we build on information integration theory and investigate the impact of certification authorities' reputation and the quality level of an audit on customers' perceived privacy within a professional cloud environment by using an experimental design including 43 professional cloud decision makers. We show that certification authorities' reputation does not alone produce opinion change, it rather affects cloud customers' perceived privacy resulting from the quality level of an audit. Our findings have theoretical implications for the information integration theory and assurance seal research. We also discuss the managerial implications of our work for CSPs and certification authorities.

Table 4 summarizes the embedded publications within this thesis.

No.	Authors	Title	Outlet	Type
P1	Lang, Wiesche, Krcmar	Conceptualization of Relational Assurance Mechanisms – A Literature Review on Relational Assurance Mechanisms, Their Antecedents and Effects	WI 2017 (accepted)	CON (VHB: C)
P2	Lang, Wiesche, Krcmar	What Are the Most Important Criteria for Cloud Service Provider Selection? A Delphi Study	ECIS 2016 (accepted)	CON (VHB: B)
P3	Lang, Wiesche, Krcmar	Criteria for Selecting Cloud Service Providers: A Delphi Study of Quality-of-Service Attributes	I&M 2018 (accepted)	JNL (VHB: B)
P4	Lang, Wiesche, Krcmar	Perceived Control and Privacy in a Professional Cloud Environment	HICSS 2018 (accepted)	CON (VHB: C)
P5	Lang, Wiesche, Krcmar	Direct Control, Institutional Control, the Power of the Market Place and Perceived Privacy: An investigation of Cloud Sourcing Projects Across Two Cultures	EJIS (under review)	JNL (VHB: A)
P6	Lang, Wiesche, Krcmar	Explaining the Impact of Cloud Assurance Seals on Customers' Perceived Privacy	ECIS 2018 (accepted)	CON (VHB: B)

CON: Conference; ECIS: European Conference on Information Systems; EJIS: European Journal of Information Systems; HICSS: Hawaii International Conference on System Sciences; I&M: Information & Management; JNL: Journal; VHB: German Academic Association for Business Research; WI: International Conference on Wirtschaftsinformatik.

Table 4. Overview on Embedded Publications

2 Conceptual Background

2.1 Cloud Computing

Triggered by the progressive adoption of CC paradigm, organizations changes how to manage their information technology (IT) landscape and IT governance (Armbrust et al. 2010). CC "is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources" (Mell/Grance 2011). Computer resources refer to hardware (IaaS), development platforms (PaaS), and applications (SaaS), and they "can be rapidly provisioned and released with minimal management effort or service provider interaction" (Mell/Grance 2011). Therefore, CC promises lower cost, increasing productivity and IT elasticity advantages, and enables new business models and values for cloud customers as well as CSPs (Morgan/Conboy 2013).

2.1.1 Cloud Computing as a Specific Form of IT Outsourcing

According to Chen/Wu (2013), from a customer's point of view CC can be seen as an evolutionary development and specific form of ITO and they share basic principles, benefits, and challenges. First, cloud customers leverage the provider's expertise and infrastructure to run a business which in turn relies on the principle of ITO (Chen/Wu 2013). Second, both CC and ITO benefit from cost savings, access to specialized resources, and the enabled flexibility to respond quickly to market changes (Schneider/Sunyaev 2016; Leimeister et al. 2010; Benlian/Hess 2011). Third, CC and ITO customers are challenged to select optimal provider to ensure ex-post sourcing performance (Garrison et al. 2012; Jain/Thietart 2013; Agrawal et al. 2006).

However, even if CC is an evolutionary development of ITO, different characteristics between ITO and CC exist and therefore CC has to be considered as a specific form of ITO. Table 5 illustrates characteristics of ITO and CC within certain dimensions: *delivery model, scope, contract, and arrangement*. CC is technology-enabled outsourcing via the internet *(delivery model*), based on standard interfaces and functionalities (*scope*) that are available to all user firms (*delivery model*) (Chen/Wu 2013; Mell/Grance 2011). Traditional ITO, on the other hand, often entails the transfer of human and physical assets (*delivery model*) and services are customer-tailored (*scope*) and available to dedicated firms (*delivery model*) (Xin/Levina 2008; Susarla et al. 2003; Linstone/Turoff 1975; Chen/Wu 2013). As a result, ITO usually involves long-term contracts while CC involves flexible short-term contracts with consumption-based pricing models (*contract*) (Schneider/Sunyaev 2016; Benlian/Hess 2011; Dongus et al. 2014). Hence, CC arrangements are best described as market-based arrangements, while traditional outsourcing arrangements are best described as hierarchical arrangements (*arrangement*) (Gurbaxani/Whang 1991; Chen/Wu 2013).

Based on these characteristics, CC has to be considered as a specific form of ITO and different outcomes from evolutionary development results (Table 5). Because CC is technology-enabled and available to all customers' firms IT resources are better described as a commodity good and not as a source of competitive advantage anymore (Chae et al. 2014; Chen/Wu 2013). The standardization of interfaces and functionalities enables customers to adopt cloud services without facing up-front investments (Susarla et al. 2003; Xin/Levina 2008). At the same time, CSPs are able to rapidly provide and release cloud services for new customers with minimal management effort (Mell/Grance 2011). The contractual mode of cloud services with short-term contracts enables customers to switch between providers more often if not satisfied with the service (Schneider/Sunyaev 2016; Benlian/Hess 2011; Dongus et al. 2014). Finally, within a market-based arrangement, customers face operational (transactional) and contractual (writing contracts) costs when selecting CSPs (Gurbaxani/Whang 1991; Chen/Wu 2013; Xin/Levina 2008).

Dimension	Characteristics of ITO	Characteristics of CC	Outcomes from evolutionary development of CC	Source
Delivery Model	Often entails transfer of human and physical assets available to dedicated customers' firms	Technology-enabled outsourcing via the internet available to all customers' firms	Commoditization of IT resources leads to equalization of competitive advantages regarding used IT.	(Chen/Wu 2013; Chae et al. 2014)
Scope	Customer-tailored services	Standard interfaces and functionalities	No up-front investments for new customers are necessary for both customer and CSP.	(Xin/Levina 2008; Susarla et al. 2003; Mell/Grance 2011)
Contract	Long-term contracts (fixed or time and material pricing models)	Short-term contracts (consumption-based pricing models)	Enable customers to switch between providers more often if necessary.	(Schneider/Sunyaev 2016; Benlian/Hess 2011; Dongus et al. 2014)
Arrangement	Hierarchical arrangement	Market-based arrangement	Customer faces operational (transactional) and contractual (writing and enforcing contracts) costs when selecting CSP.	(Gurbaxani/Whang 1991; Chen/Wu 2013; Xin/Levina 2008)

Table 5. Outcomes from evolutionary development of cloud computing (adopted from Lang et al. (2016))

2.1.2 Cloud Sourcing Process

Conducting decisions on cloud sourcing is a complex process involving three consecutive steps (Luoma/Nyberg 2011; Zhou et al. 2007; Moe et al. 2017). These steps include the cloud sourcing decision itself, pre-qualification of possible CSPs, and CSP selection (Figure 6).

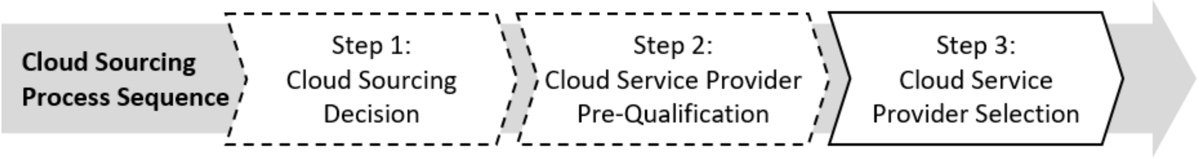

Cloud Sourcing Process Sequence
Step 1: Cloud Sourcing Decision
Step 2: Cloud Service Provider Pre-Qualification
Step 3: Cloud Service Provider Selection

Figure 3. Cloud sourcing process (Step 3 is the focus of this thesis) (adopted from Lang et al. (2018a))

In the first step, cloud customers make a decision on cloud sourcing. Inhibiting and facilitating factors for cloud sourcing affect this decision-making (Benlian/Hess 2011; Oliveira et al. 2014). While an increasing strategic importance of services, available risks, or perceived complexity may prevent cloud customers to cloud source services, the possibility to save costs, access specialized resources, increase flexibility, or reduce time to market facilitates cloud customers to cloud source services (Schneider/Sunyaev 2016; Luoma/Nyberg 2011). Both facilitating and inhibiting factors influence cloud customers to cloud source their services within the initial decision-making step.

In the second step, cloud customers preselect possible CSPs depending on functional requirements and boundary restrictions (Schneider et al. 2018). Only providers that serve required service models (IaaS, PaaS, or SaaS providers) and needed functions or applications (CRM system) are considered (Garg et al. 2013; Schrödl 2012). Boundary restrictions on the data, e.g., sensitive data that are liable to specific regulatory requirements such as accounting systems constitute the list of preselected CSPs (Rieger et al. 2013; Zhou et al. 2007). This list of CSPs might fulfill the purpose of the cloud sourcing endeavor (Garg et al. 2013; Schrödl 2012). The challenge is to discover the “right” CSP that is required by the cloud customer to conduct a detailed CSP examination within the next step (Garrison et al. 2012; Garrison et al. 2015; Weinhardt et al. 2009).

Cloud customers have to select an appropriate CSP, the third step in the decision-making process. Often several CSPs fulfill basic requirements regarding required service model, required functions, or applications (Garg et al. 2013). In addition to functional requirements and boundary restrictions, QoS requirements must be considered (Garg et al. 2013). As an example, CSPs warrant different levels of availability usually varying between 98% and 99.999%. Cloud services have a high diversity of different QoS attributes (Ghosh et al. 2015); cloud customers have to select from a plethora of offerings and decide which QoS attributes are relevant and which provider can fulfill their QoS requirements (Huang/Nicol 2013).

2.1.3 Information Privacy and Privacy Risks in Cloud Sourcing Projects

Information privacy refers to the concept of controlling how sensitive business information is acquired and used (Pavlou 2011). Privacy has been exhaustively studied since 1945 and the privacy concept followed the evolution of IT (Westin 2003). Between 1945 and 1960, limited IT developments evolved decision makers’ high trust in the business sector and general comfort with information collection and is defined as a baseline for the concept of privacy (Pavlou 2011). After this time, privacy ran through three eras (1961–1979; 1980–1989; and 1990–present) in which emerging technologies (mass production, rise of computer and network systems, and rise of the internet and related technologies, respectively) shaped the concept of privacy (Pavlou 2011).

A major development in the third era, for example the rise of CC, was the globalization of the privacy issue driven by rising dependencies on third parties (Westin 2003). Clients use global resources (hardware, platforms, or applications) on-demand across the globe to gain advantages such as decreasing costs (Schneider/Sunyaev 2016). However, an information asymmetry exists between decision makers who are responsible for clients' decisions and technology providers who implement privacy control mechanisms. The cause of this asymmetry is the power of the provider who possesses superior information about their capabilities and willingness to keep sensitive information private or appropriate a surplus value. After the maturity of the ITO market increased, privacy risks decreased (Schermann et al. 2016). Nevertheless, the cloud sourcing market is still an emerging market in which decision makers face privacy risks like the risk of shirking and poaching (CSA 2016).

ITO literature suggests that shirking and poaching are strategic risks since they are caused by actions that providers may initiate deliberately as part of a profit-maximizing strategy (Clemons/Hitt 2004). As cloud sourcing involves the possibility and risk of shirking and poaching tremendously increases due to the large volume of worldwide data exchange, storage, and processing possibilities of information. Should shirking or poaching occur, the existing information asymmetry prohibits a client from knowing or being able to identify the source of the superior information in the possession of the third party. Shirking and poaching do not necessarily immediately harm the client but can embarrass them and cause a long-term effect by damaging reputational capital. Hence, the detection of these privacy risks is difficult.

2.2 Privacy Fundamentals

Privacy has been conceptualized in a variety of ways, such as (1) perceived state of privacy; (2) privacy as control in which individuals have the ability to control transactions between individuals and others; and (3) a combination of these (Smith et al. 2011). While control is an important factor in forming individuals' privacy perception, it is not identical to privacy itself (Dinev et al. 2013). Therefore, while we focus on a perceived privacy per se, we consider the influence of control perception on the perceived privacy simultaneously.

2.2.1 Perceived Privacy

In an online environment, a perceived state of privacy (short perceived privacy) refers to an aggregation of consumers' perceptions and expectations regarding a provider's characteristics when storing or processing sensitive information (Chellappa 2008; Frye/Dornisch 2010). A group of scholars (Bansal et al. 2015; Smith et al. 1996) includes customers' perceptions regarding collection and subsequent access, use, and disclosure of sensitive information as representative characteristics that influence one's privacy perceptions. Collection refers to what sensitive information a provider collects from a customer. Access refers to whether or not reasonable steps are in place to assure that sensitive information is accurate and secure from unauthorized use. Unauthorized use refers to whether or not sensitive information will be used for purposes other than those for which they have been provided. Disclose refers to whether or not sensitive information is disclosed to secondary parties. Perceived privacy results when consumers compare the actual and expected collection and subsequent access, use, and disclosure of their sensitive information (Chellappa 2008; Frye/Dornisch 2010).

Therefore, perceived privacy reflects the amount of consumers' belief that the institutional setup allows for the privacy of their transaction to be maintained as promised. Perceived privacy is defined as "an individual's self-assessed state in which external agents have limited access to information" (Smith et al. 2011).

2.2.2 The Influence of Perceived Control on Perceived Privacy

Perceived control is more powerful to influence customers than actual control. According to Johnson (1974), individuals use control to attain privacy-related outcomes. In psychology, the construct of control has been treated as a perceptual construct because it is of greater interest than actual control when predicting behavior (Skinner 1996). The conceptualization of perceived control is therefore a cognitive construct, and as such it may be subject to available information. Perceived control refers to an individual's beliefs regarding his or her ability to affect changes in the environment in a desired direction (Smith et al. 2011).

Perceived control influence customers' perceived privacy. Privacy enhancing features can provide customers with means of control the disclosure, access, and use of sensitive information and, thus, increase the level of perceived control (Xu et al. 2012b). Consumers tend to have higher privacy perceptions when they believe that they have a higher level of perceived control over the disclosure and subsequent use of their information in a specific situation (Dinev et al. 2013). Hence, perceived control over information determines the customers' level of perceived privacy.

2.2.3 Control Agents Influence Consumers' Perceived Privacy

Privacy perceptions and the intentions of cloud customers are influenced by three different control agents, namely personal control, proxy control, and collective control (Xu et al. 2012b; Yamaguchi 2001):

The personal control approach aims to directly assure outcomes from a cloud customers' perspective. People experience greater autonomy when they exercise direct personal control as the assurance agent (Yamaguchi 2001; Johnston/Warkentin 2010; Xu et al. 2012b). Such control empowers individuals with mutual control over how their data and information, for example, may be used by CSPs via technological and non-technological self-protection approaches (Xu et al. 2012b; Yamagishi/Yamagishi 1994). By using personal control, actors induce the partner to take a certain course of action with the use of strategies such as "tit-for-tat" (Axelrod/Hamilton 1981; Wang et al. 2008; Xu et al. 2011). Using these strategies, actors match their own behaviors to those displayed by personal control mechanisms (e.g., cooperating or trustful versus competing or opportunistic) (Axelrod/Hamilton 1981).

The proxy control approach aims to indirectly assure outcomes via powerful others (Son/Kim 2008; Hui et al. 2007; Tang et al. 2008). Institutional mechanisms are used from partners with few resources or low power to gain assurance through skillful and powerful third parties (e.g., certification authorities or legislation) (Bandura 2001; Yamaguchi 2001). These mechanisms enable partners to access resources from third parties, such as knowledge and power, to assure outcomes. In case of opportunistic behavior, these assurance structure provides mechanisms of voice and recourse for the betrayed, which could create strong incentives for firms to refrain from opportunistic behavior and behave appropriately (Benassi 1999; Xu et al. 2011; Shapiro et al. 1992).

In the collective control approach, an individual, as a member of a group or collective that serves as an assurance agent, attempts to control the environment or outsiders. In collective control, responsibility, as well as agency, will be diffused among actors (Latané/Darley 1970). In the collective control approach, individuals attempt to share responsibilities among actors, internalize reference groups, and use their collective knowledge for decision-making (Venkatesh et al. 2003; Yamaguchi 2001). Therefore, the collective is responsible for possible positive and negative outcomes to the same extent (Yamaguchi 2001).

Research should consider all three control agents when investigating privacy perceptions of decision makers. Table 6 summarizes the factors which influence cloud customers' perceived privacy.

Control agent	**Controller**	**Control mechanism example**
Personal control	Individuals	Monitoring, privacy policy
Proxy control	Powerful authorities	Certification, legislation
Collective control	Collective	Reputation

Table 6. Control agents who influence cloud customers privacy perceptions (adopted from Lang et al. (2017))

2.2.4 The Effect of Cultural Differences in Uncertainty Avoidance on Perceived Privacy

Risk perceptions influence individual decision makers. In a company, individuals are responsible for decision-making. Therefore, a client's decisions are likely to be shaped to some extent by the cultural background of the decision maker.

A cultural factor related to risk perceptions like perceived privacy risks is uncertainty avoidance, defined as the extent to which people of a culture feel threatened by unknown situations (Keil et al. 2000). A decision maker's disposition to avoid uncertainty influences perceptions and risk behavior (Srite/Karahanna 2006). As an example, opportunistic behavior in low uncertainty avoidance cultures is likely since they do not fear the future (Nakata/Sivakumar 1996). As a consequence, these cultures distrust other people and providers because they expect others to also initiate opportunistic behavior and put special emphasis on their own abilities (Doney et al. 1998; Xu et al. 2012b). By contrast, high uncertainty avoidance cultures are more willing to share knowledge and are influenced by social norms (Srite/Karahanna 2006). In these cultures, decision makers expect the same behavior from their vendor who aims to have high reputational capital. In such cultures, subjective norms contribute to reducing uncertainty and opportunism (Dinev et al. 2009; Srite/Karahanna 2006). Therefore, uncertainty avoidance differs among decision makers and affects what control mechanisms decision makers prefer.

3 Research Approach

3.1 Research Strategy

3.1.1 Philosophical Perspectives and Research Epistemology

Every research endeavor is based on general underlying assumptions about what constitutes "valid" and "good" research and which research methods are appropriate. Those philosophical assumptions are related to the underlying epistemology that guides the research. In general, epistemology refers to the assumption about knowledge and how it can be obtained (Hirschheim 1985).

While a detailed analysis and examination of various epistemological approaches (see Tschamler (1996) or Guba/Lincoln (1994)) is beyond the focus of this thesis, the three-fold classification (positivist, interpretive, and critical) of (Orlikowski/Baroudi 1991) is adopted here as it is one of the most appropriate overviews of the underlying epistemological perspectives and assumptions in IS research (Myers 1997). However, more recently, a fourth position, pragmatic research, has evolved (Creswell 2009). Therefore, this thesis describes these four positions along their beliefs about reality, knowledge, and the relationships between theory and practice (Chua 1986; Orlikowski/Baroudi 1991). Beliefs about reality concern questions about the objectivity of reality, human intentionality, and the stability of social relations. Beliefs about knowledge concern questions about the criteria for generating knowledge and the validity of research methods for doing so. Beliefs about the relationship between theory and practice concern questions about the purpose of knowledge in practice.

> **Positivist Research.** Positivist research is dominant in behavioral IS research (Orlikowski/Baroudi 1991). It is the view that objects have an existence independent of the knower (Cohen et al. 2013). The positivist position assumes an objective physical and social world in which the researcher can discover the objective physical and social reality by using the right methods of data collection and analysis. The positivist perspective assume that human action is intentional and rational. The assumption about social reality is that humans interact in relatively stable and orderly ways (Orlikowski/Baroudi 1991). In regard of beliefs about knowledge, the positivist perspective is concerned with the empirical testability of theories, whether to verify or falsify those. Applying the hypothetic-deductive model based on hypotheses or prediction helps researcher to test theories (Chua 1986). Regarding the relationship between theory and practice, positivist research approach is that the researcher is independent of the phenomena being studied, and hence assumes a value-neutral stance. The researcher can objectively evaluate phenomena being studied, but should not get involved in moral judgements or subjective opinion (Orlikowski/Baroudi 1991).
>
> **Interpretive Research.** Interpretive research is the view that reality is subjective and differs from person to person (Guba/Lincoln 1994). The interpretive position assumes an interpretive perspective emphasizing the importance of subjective meanings of the researcher. It aims to understand how individuals adjust their social actions according their knowledge and how they reconstruct their reality (Orlikowski/Baroudi 1991). In

regard to beliefs about knowledge, the interpretive philosophy is contradict to the positivist philosophy and the social world can only be understood from the standpoint of individuals who are participating in it (Cohen et al. 2013). Therefore, the interpretative methodology is directed at understanding phenomenon from an individual's perspective, investigating interaction among individuals, technologies or organizations (Creswell 2009). Consequently, appropriate methods for generating knowledge study phenomena of interest in their natural context and do not required to generalize their findings (Orlikowski/Baroudi 1991). With regard to its beliefs about the relationship between theory and practice, interpretive research beliefs the researcher cannot be assumed value-neutral since he is connected to the phenomenon under investigation. Researchers tend to influence the research process through their personal beliefs, values, assumptions, and interests (Orlikowski/Baroudi 1991).

Critical Research. Critical research is the view that social, political, cultural, economic, ethnic, and gender values shape reality; reality that was once deemed plastic has become crystallized (Guba/Lincoln 1994). The critical position assumes that criteria for judging theories are temporal and limited by the environmental context. In regard to the beliefs about knowledge, critical research assumes that knowledge is grounded in social and historical practices and requires an in-depth understanding of the phenomenon of interest including historical development and is contemporary context and contradictions (Chua 1986). Thus, critical research goes beyond the interpretive research by also considering conditions, which lead the researcher to interpretations. With regard to its beliefs about the relationship between theory and practice, the critical research beliefs that theory needs to point out contradictions of reality to actively effect change in the phenomena being investigated (Orlikowski/Baroudi 1991).

Pragmatic Research. Pragmatic research rejects the preoccupation with theory of other epistemological positions and their disregard for the way scientists actually work. The pragmatic position assumes that there exists a reality independent of the observer (Creswell 2009). However, pragmatists do not mainly focus on questions concerning the nature of reality (Cherryholmes 1992). Moreover, pragmatists are also skeptical of individuals' ability to grasp reality in an objective way and, therefore, focus on whether the actions taken based on individuals' conception of reality led to the desired results (Cherryholmes 1992). In regard to the belief about knowledge, pragmatists assume that knowledge relates to the actions that are used to cope with specific situations and the consequences of these actions (Johnson et al. 2007). Consequently, acceptable methods for generating knowledge can be either quantitative or qualitative and depend on the phenomena being investigated (Creswell 2009). With regard to beliefs about the relationship between theory and practice, pragmatisms belief theory and practice are closely connected and theory is essential for achieving an informed practice (Cherryholmes 1992).

3.1.2 Strategies of Inquiry

Strategies of inquiry describe types of research methods that move from the underlying philosophical assumption to the research design and collection of data (Myers 1997). The choice of research method thus highly affects the way the researcher collects data. Three different strategies of inquiry exist in behavioral research (Creswell 2009): Qualitative strategies, quantitative strategies, and mixed strategies.

Qualitative strategies. Qualitative research aims to understand and explain rare and/or complex social and organizational phenomena. Based on complexity and rarity of the investigated phenomena, qualitative research is often limited to a number of units that are analyzed and do not aims to generalize the results (Strauss/Corbin 1990). Qualitative research is independent from the underlying epistemological position and, therefore, can rely on positivist, interpretive, critical, or pragmatic (Myers 1997). The phenomena under investigation get analyzed using qualitative data, such as interviews, documents, and participant observations (Myers 1997). The researcher gets in an intense contact with real life situations and tries to generate an in-depth understanding of how the actors perceive and manage these situations. Prominent examples of qualitative research methods in the IS context are grounded theory (Wiesche et al. 2017) or case study research (Yin 2013).

Quantitative strategies. Quantitative research aims to understand and interpret quantitative data for which a limited number of variables of interest are available (Straub et al. 2005). Therefore, in contrast to qualitative research, which aims to understand the meaning and the context, quantitative research aims at generalization from samples to the populations of interest. Quantitative research is limited to the epistemological positions of positivist and pragmatic to choose from, since it aims reliable and from the researcher independent and generalizable results (Straub et al. 2005). To assure generalizable results, the researcher differentiate between criteria relating to instrumentation validity, criteria relating to internal and external validity, and criteria relating to statistical conclusion validity (Straub et al. 2004). The phenomena under investigation get analyzed using quantitative data, such as archival data, data gathered through a survey or through experiments. The researcher is motivated by the numerical outputs and how to derive meaning from them (Straub et al. 2005).

Mixed strategies. Mixed strategies aims to combine the strengths of qualitative and quantitative strategies by combining both to collect and analyze data (Johnson et al. 2007). Consequently, mixed strategies allow researchers to better address exploratory and confirmatory research at the same time, to provide stronger inferences, and to generate a richer understanding of the phenomenon of interest than either a qualitative or a quantitative strategy on its own (Venkatesh et al. 2013). Three different approaches exist for mixed strategies (Creswell 2009): concurrent, sequential, and transformative. Concurrent approaches collect and analyze quantitative and qualitative data in parallel and integrate both analyses into overall findings. Sequential approaches collect and analyze qualitative and quantitative data in parallel and integrate both analyses into overall findings. In the transformative approach, the researcher uses a theoretical lens, which guide either a concurrent or a sequential mixed strategy.

3.1.3 Summary of Epistemological and Strategies of Inquiry of this Thesis

With the foundations of epistemological positions and strategies of inquiry in mind, this thesis can be described closest as pragmatic based on a mixed strategy to investigate relational assurance mechanisms from a cloud decision maker's perspective. Dependent on which fits best to the research problem at hand and which is likely to maximize our understanding of the phenomenon in question, this thesis follows a mixed strategy and, therefore, draws on both quantitative and qualitative research methods. Consequently, we share pragmatism's pluralistic stance. Moreover, we identify with pragmatism's focus on consequences. Throughout this thesis, we emphasize the importance of the practical implications of our research results, which aims to increase privacy perception building and cloud service adoption.

3.2 Research Methods

Following the pragmatic paradigm and a mixed strategy of inquiry, this thesis employs both, qualitative and quantitative research methods. The next section briefly introduces the methods and related characteristics used in this thesis. The respective papers describe the procedures in detail.

3.2.1 Literature Review

"Understanding the past to prepare for the future" (Webster/Watson 2002) is essential for any successful academic research project (Iivari et al. 2004). Literature reviews represent a systematic approach to do so by investigating relevant studies and their results pertaining to a particular focus and goal of a literature review (Cooper 1988). Foci of literature reviews may include research outcomes, research methods, theories, or applications while goals may comprise integrating and synthesizing prior work, criticizing it, or identifying central issues (Cooper 1988). The results of a literature review should list the identified literature, conceptualize their results, and discuss possible direction for future research (Webster/Watson 2002).

Important steps in a literature review comprise:

Searching for relevant publications. Literature reviews differ in terms of their exhaustive, representative, or pivotal coverage of literature (Cooper 1988). An exhaustive coverage aims at including all publications relevant to the underlying research questions. A representative coverage chooses a sample that is deemed characteristics for a larger group of publications and makes inferences from the sample to that group. The pivotal coverage focuses on publications that are considered central to the topic of interest. With regard to coverage, research should use an exhaustive coverage following a systematic, three-step approach to identify relevant publications (Webster/Watson 2002). First, a key-word based search in leading journals and conference proceedings of the field employing electronic databases is recommended. The key-word search should be complemented by a manual scan of journals' and conference proceedings' tables of content to make sure that all relevant studies in the leading publications outlets have been identified. Focusing on leading publication outlets helps to ensure the quality of the obtained results (Vom Brocke et al. 2009). Second, the researcher should conduct a backward search. The backward search enables to consider prior work that is cited in the identified articles. Third, a forward search assures that the literature review also considers articles that cite the identified articles. The search for relevant literature is complete when no new arguments, methodologies, findings, concepts, and authors relevant for the focus and goal of the literature review can be found (Webster/Watson 2002).

Structuring and synthesis of the review. After identifying the sample population of the literature review, the publications should be structured and analyzed according the underlying focus and goal of the literature review. Two different approaches exist for the structuring and analysis of the review: author-centric and concept-centric (Webster/Watson 2002). While the author-centric approach rather provides a list of relevant publications without a proper synthesis, the concept-centric helps "to assemble the literature being reviewed for a given concept into a whole that exceeds the sum of its parts" (Levy/Ellis 2006). Therefore, the concept-centric approach should be preferred over the author-centric approach. The transition from an author- to a concept-centric review can be accomplished with the help of a concept matrix (Salipante et al. 1982).

3.2.2 Delphi Study

The objective of most Delphi studies is the reliable and creative exploration of ideas or the production of sustainable information for decision-making (Pare et al. 2013). The Delphi method is a structured process of collecting and distilling knowledge from a panel of experts by means of questionnaires interspersed with controlled opinion feedback (Adler/Ziglio 1996). Delphi studies employ multiple iterations of questionnaires and feedback to develop a consensus of opinion that concerns a particular problem or topic (Schmidt et al. 2001). The process is viewed as a series of rounds, and in each round, participants communicate their opinions through a questionnaire that is returned to the researchers, who collect, edit, and return to every participant a statement of the position of the panel and the participant's own position (Schmidt 1997). Thus, the Delphi method represents an inductive and data-driven approach that is often used in exploratory studies when empirical evidence exists (Pare et al. 2013).

The Delphi method was developed by the Rand Corporation in the 1950s and early 1960s as a methodology that was used for the elicitation of experts opinions in the domain of long-range forecasting (Gordon/Helmer 1964). Nowadays, the Delphi method has been used in a variety of fields such as the physical science, engineering, education, business and economics, as well as in IS research (Pare et al. 2013). The Delphi method continues to contribute to the IS field through its unique method of accessing knowledge that is embedded in years of hands-on IT practitioners' expertise. It has been used to study IT outsourcing (Nakatsu/Iacovou 2009) and software project risk management (Schmidt et al. 2001).

Important steps in the Delphi study include:

Selecting the experts. Studies employing the Delphi method make use of experts who have knowledge of the topic being investigated (Pare et al. 2013). The inclusion of a panel of experts is based on the rational that the pool intelligence of a group of experts is better than one expert when exact knowledge on a topic is not available (Schmidt 1997). The selection of the right panel of experts is the most critical factor in the success of a Delphi study as this depends on their collective expertise.

Studies applying the Delphi method usually use non-random, purposive samples (Schmidt et al. 2001). The sample selected when employing such a survey is referred to as the "panel of experts" (Schmidt et al. 2001). Purposive sampling refers to the sample being selected purposely and depends on the researcher's judgment, in line with the aim of the study, regarding whom she/he judges to be typical of the population and is particularly knowledgeable about the issues being studied.

Regarding the panel size, there are no clear guidelines suggesting the numbers to be included in studies applying the Delphi method because the sample is purposively selected, and depends on the problem being investigated. While larger samples are preferable to smaller ones as individual misjudgments are compensated for, the quality of experts should be prioritized over quantity to assure validity of the results (Häder/Häder 1994).

Consulting the experts. During the actual Delphi study, three phases are typically conducted: brainstorming phase, narrowing down phase, and ranking phase (Pare et al. 2013). The brainstorming phase is unstructured and asks individuals to respond to broad questions. This phase gives experts the freedom to list the items that they think are important for the chosen area of interest. After the experts' responses have been received, the researcher attempts to eliminate redundancy and creates a single list of items. The resulting list is used to produce a questionnaire for the subsequent rounds. Since individuals have cognitive limitations to rank different items, a narrowing down phase is required (Schmidt et al. 2001). This phase is narrows down the list of items that was developed during the brainstorming phase to a number that is reasonable and manageable for the ranking in the third phase. To accomplish this process, the researchers send the list back to the experts along with instructions to indicate those items that are most important. At the end of this phase, the number of items should be between 12 and 15 (Singh et al. 2009). The aim of the ranking phase is to reach a consensus in the ranking of the selected items. Reaching consensus may involve several rounds of collecting and analyzing the experts' ranking. This phase ends, when a reasonable level of consensus or another pre-defined stop-criterion is achieved (Schmidt 1997).

Analyzing the results. Depending on the research question, there are various elements that should be part of the analysis. For ranking type Delphi studies the identification, the selection, and the ranking in the different rounds should be part of the analysis (Schmidt 1997). First, it should be analyzed which items were identified from the overall panel. This might give insights of new identified or frequently mentioned items in the literature. Second, the analysis should elaborate on which items were deemed to be important. This provides insights about which items exist overall and which of them are important regarding the research topic. Last, the relative importance of the items within and between the possible different rounds and the level of consensus within each round should be investigated. The level of consensus is typically investigated using Kendall's W (Schmidt 1997).

3.2.3 Survey Research

Survey research aims to obtain information by gathering data from a particular sample of a given population, through personal or impersonal means, to study its characteristics (Isaac/Michael 1995). It consists of three principal characteristics (Kraemer/Dutton 1991): First, survey research is used to quantitatively describe specific aspects of a given population. These aspects often involve examining the relationships among dependent and independent variables. Second, the data required for survey research are collected from people and are, therefore, subjective. Finally, survey research uses a selected portion of the population from which the findings can later be generalized back to the population.

In survey research, independent and dependent variables are used to define the scope of a study, but cannot be explicitly controlled by the researcher. Before conducting the survey, the researcher must predicate a model that identifies the expected relationships among these variables. The survey is then constructed to test this model against observations of the phenomenon.

Survey research can be used for exploration, description, or explanation purposes. The purpose of survey research in exploration is to become more familiar with a topic and to try out preliminary concepts about it. The purpose of survey research in description is to find out what situations, events, attitudes or opinions are occurring in a population. The purpose of survey research in explanation is the most common in IS research and aims to test theory and causal relations.

Important steps in the survey research include:

Survey design. A research design is the strategy for answering the questions or testing the hypotheses that stimulated the research in the first place. Survey designs may be distinguished as cross sectional or longitudinal, depending upon whether they exclude or include explicit attention to the time dimension (Pinsonneault/Kraemer 1993). The classic cross-sectional design collects data at one point in time from a sample selected to represent the population of interest at that time. The classic longitudinal design collects data for at least two points in time.

Another critical issue in research design is determining the unit(s) of analysis, or the unit about which statements are being made. Different units of analysis are possible in a survey but must be related to the questions and hypotheses in the research.

Finally, the design for data analysis is important. The analysis of survey research, which focuses on exploration or description, frequently involves no more than developing the marginal- and cross-tabulations for the variables and using simple descriptive statistics such as means and medians (Pinsonneault/Kraemer 1993). When explanation is the aim, analysis must employ the full logic of survey analysis (Babbie 1973). That logic is illustrated by testing hypotheses with cross-sectional data.

The use of cross-sectional survey data to test causal hypotheses requires that the investigator designs the survey to include data on the independent and dependent variables (Pinsonneault/Kraemer 1993). The analysis, then, involves introducing these antecedent variables into the two-variable (or more) relation to test the null hypothesis. Testing causal relationships with cross-sectional designs in this manner is only possible when very specific factual data that can be correctly remembered by informants are used (Pinsonneault/Kraemer 1993).

Sampling procedures. Sampling is concerned with drawing individuals or entities in a population in such a way as to permit generalization about the phenomena of interest from the sample to the population (Kraemer/Dutton 1991). The most critical element of the sampling procedures is the choice of the sample frame. It constitutes a representative subset of the population from which the sample is drawn. The sample frame must adequately represent the unit of analysis (Babbie 1973).

Data collection. Regardless of the unit of analysis, the units for data collection in survey research are usually individuals. Individual responses are often aggregated for larger units of analysis such as role, work group, department, or organization (Babbie 1973). Depending upon the phenomena under investigation, it may be sufficient to have a single individual as respondent for each of these units of analysis (Pinsonneault/Kraemer 1993). More often, however, it is necessary to have several individuals as respondents because people function in different roles and at different levels of the hierarchy and, consequently, have differing experiences and perceptions of the technology and its impacts in the organization (Pinsonneault/Kraemer 1993). Therefore, it is not only important to determine exactly what is the unit of analysis, but also who will be the respondents representing the unit of analysis of interest. Once this is determined, most sampling issues are straightforward (Babbie 1973).

The choice of data collection method, such as mail questionnaire, telephone interviews, or face-to-face interviews, is significant because it affects the quality and cost of the data collected (Kraemer/Dutton 1991). In general, quality and cost are highest with face-to-face interviews or telephone interviews whereas quality and cost are lower with mail questionnaires and group administration.

3.2.4 Free Simulation Experiments

The aim of experimentation is to identify cause-effect relationships, and it consists of three principal characteristics: First, the experimenter does not wait until a specific event occurs, but creates a specific treatment, which resembles the desired event. Second, the experimenter controls the source of the variation. As a result, changes in the behavior of the participants can be traced back to the variation caused by specific treatments. Third, the experimenter needs to ensure to choose an environment that allows him to precisely measure the variables. Whereas standard laboratory experiments rely on a treatment to vary one or more independent variables, free simulation experiments expose the participants to a number of realistic events during a specific amount of time. One core feature of free simulation experiments is that the realistic events are designed by the experimenter, but due to the feature that they are free to behave in certain boundaries the participants could create additional realistic events on their own (Fromkin/Streufert 1976).

As experiments are conducted in an artificial laboratory environment, a high internal validity (allowing the identification of cause-effect relationships instead of correlations) exist. However, laboratory experiments are often criticized for their lack of external validity (allowing to conclude that the observed results will hold in a real-world setting) (Fromkin/Streufert 1976). Since free simulation experiments simulate realistic event, they provide a good trade-off between internal and external validity of the results.

Important steps in the free simulation experiment method include:

> **Experiment design.** A guiding principle in setting up experiments is simplicity (Smith 1976). The rationale behind a simple design is that, with a parsimonious setup, the researcher can attribute the differences in observations to the manipulations of the experimental environment. The need for a parsimonious design led to another salient feature of experiments, which is that abstractions from realistic context are permitted (Ariely/Norton 2007).
>
> Another critical issue is the choice between a within- and between subject design. A within-subjects design differs from a between-subjects design in that the same subjects perform at all levels of the independent variable. A within-subject experimental design controls for subject variability (it accounts for individual differences when subjects serve as their own control) (Keppel 1991). In addition, a within-subject design provides the opportunity to simulate repeated decisions, a frequently occurrence in real life (Andriole 2007). Contrary, in a between-subjects design, the various experimental treatments are given to different groups of subjects. While such a setting increases the reliability of the results by avoiding learning effects, it also ignores possible differences among the subjects.
>
> **Choice of the subject pool.** Researchers can use either a sub-sample from the target population or use proxies like students to investigate the research topic. Many of the laboratory experiments in IS involve students from academic institutions (Gupta et al. Forthcoming 2018). However, it is likely that the cardinal measures of outcomes differ depending on the population (student versus professional), or cultural differences for instance (Gupta et al. Forthcoming 2018). In particular, care must be taken as certain knowledge is required during the experimental tasks (Lowry et al. 2012). Contrary, when focusing on ordinal measures of policies, the sampling strategy becomes less relevant (Lichtenstein/Slovic 1973).

Data collection. Once the main structure of the experiment is decided, the focus shifts to the following three main issues: a) input to the experiment; b) activities during the experiment; and c) conclusions from the experiments (Gupta et al. Forthcoming 2018): The most important aspect regarding the input to the experiment is how subjects are engaged in the experiment. Therefore, both the incentive structure and realistic tasks are required. Activities during the experiment involve the treatments. Treatments are applied to experimental units in the treatment group(s). Most experiments also apply a control group having no treatment as a baseline. To assure the validity of experimental outcomes, experiments frequently conclude with a demographic survey to elaborate the generalizability of the outcomes.

Part B

4 Conceptualization of Relational Assurance Mechanisms

Title	Conceptualization of Relational Assurance Mechanisms – A Literature Review on Relational Assurance Mechanisms, Their Antecedents and Effects
Authors	Lang, Michael* (michael.lang@in.tum.de) Wiesche, Manuel* (wiesche@in.tum.de) Krcmar, Helmut* (krcmar@in.tum.de) *Technische Universität München, Chair for Information Systems, Boltzmannstraße 3, 85748 Garching, Germany
Publication	International Conference on Wirtschaftsinformatik (WI)
Status	Accepted
Contribution of First Author	Problem Definition, Research Design, Data Analysis, Interpretation, Reporting

Table 7. Fact Sheet Publication P1

Abstract

Assurance mechanisms are an important element of relational governance and frequently used in information systems (IS) research; still missing in this field, however, is a coherent and interrelated structure to organize available knowledge. In this study, we provide a first step towards development of a conceptualization framework of relational assurance mechanisms to enable their further investigation. From our analysis of existing literature, we discover two gaps in assurance research: (1) a fragmentation of assurance research and (2) a lack of conceptual consensus on relational assurance mechanisms. We provide a theoretical framework consisting of a conceptualization of identified relational assurance mechanisms, their antecedents and effects as a means of advancing theory in this area. Several possibilities for future research are discussed.

4.1 Introduction

In recent years, relational governance of inter-organizational relationships has emerged as a dominant perspective in exchange relationships (Gopal/Koka 2012). Within information systems (IS) research, attention has been focused on how relational governance complements formal contracts in order to increase predictability in interactions or expectations within exchange relationships (Poppo/Zenger 2002).

Within the higher-order construct of relational governance, relational assurance mechanisms (RAMs), such as monitoring or reputation, are particularly known to increase predictability in interactions or expectations within (potential) exchange relationships (Noordewier et al. 1990; Dyer 1997; Gundlach/Cannon 2010). According to Yamagishi/Yamagishi (1994), assurance is defined as an expectation of benign behavior for reasons other than goodwill of the partner (Barber 1983). Hence, RAMs may be conceptualized as an important element of relational governance (Noordewier et al. 1990; Dyer 1997; Gundlach/Cannon 2010) although evidence evolving from research is lacking.

We discovered two key gaps in assurance research. Firstly, investigations related to assurance are fragmented and largely independent of RAMs and assurance as a concept. These investigations do, however, offer insights on the relationship between the antecedents and effects of RAMs. Secondly, our data shows that RAMs lack a conceptual consensus. Research is at odds when it comes to a consistent interpretation of the effects of RAMs. It is difficult to advance the theoretical and empirical investigation of RAMs, as existing literature does not provide a coherent and cumulative body of work. The gaps we discovered need to be considered when investigating RAMs as an important element of relational governance. In order to address these gaps, this article attempts to answer the following research questions (RQ). *RQ1: What mechanisms of assurance are exemplary discussed in information systems literature? RQ2: Which concepts are relevant when investigating assurance mechanisms and how are these concepts related?* To reach answers to these two questions, we conducted a systematic literature review and analyzed the results of this review in a structured manner.

Using our analysis results, we provide an overview of and conceptualize RAMs as published in IS literature. Furthermore, we point out identified concerns as the antecedents of RAMs, and the effects of RAMs on individuals within a theoretical framework.

The remainder of this article is structured as follows: In the next section, we describe the design of our literature review, including our methods for selecting journals and articles, and the subsequent analysis of the selected articles. Next, we discuss the theoretical background of our work including a psychological perspective of control as a source of assurance, and subsequently present the findings of our literature review. In the final section of the paper, we discuss our findings, address their theoretical implications and identify the limitations of this study.

4.2 Methodology

To identify relevant literature regarding our RQ1 and RQ2, we conducted a systematic literature review following the guidelines of Vom Brocke et al. (2009) for the literature search, Webster/Watson (2002) for literature analysis and synthesis, and Müller-Bloch/Kranz (2015) to identify the research gap. According to our RQ1, the primary focus of this review is IS literature, identifying the key-concepts regarding our RQs within this research domain. Hence, the initial set of possible journals was limited to IS journals. As a result, all journals of the AIS senior scholars' "basket of 8 journals" were selected. To consider upcoming research topics as well, we also included high-quality, relevant articles from IS conferences.

We scanned journals using the online literature database EBSCOhost, searching for the term *"assurance"* used in the title, abstract, or keywords. For IS conference proceedings, we used the databases AISELNET and IEEE Xplore and searched abstracts for the word *"assurance"*. Articles published before June 2016 were considered. In order to get a broad overview of the concept "assurance" within exchange relationships, the search string was not limited further. As described below, further restrictions were carried out manually as part of the check for topic relevance. Overall, we initially identified 185 articles.

The articles were screened for relevance by reading title, abstract and, if necessary, the full text. In terms of our research, article relevance was defined as: the article uses the construct "assurance" in an exchange relationship context. Therefore, our selection comprises full research articles focusing on inter-organizational relationships, relationships between organizations and people, and inter-personal relationships. We excluded articles focusing on software development or product quality assurance as those do not cover assurance within an exchange relationship context. As a result, a set of 36 articles were included in our analysis. Next, we applied backward and forward search techniques to identify additional articles relevant for our research (Vom Brocke et al. 2009). In the backward search, we reviewed the reference lists in our set of articles for appropriate articles. Similarly, we reviewed the citations of the articles in our set in Google Scholar. This final search technique yielded a final set of 52 articles.

After having identified the set of relevant articles, two researchers independently reviewed each article and developed an appropriate coding scheme. The researchers then compared their results and discussed any differences in their findings (Webster/Watson 2002). After three iterations, the researchers agreed on a final coding scheme, which was used for our analysis. This scheme included the used RAM, concerns as RAM antecedents (privacy concerns, security concerns, business integrity concerns), and the effects of the RAM on individuals (beliefs, intentions, behaviors) (Müller-Bloch/Kranz 2015). According RQ1 and RQ2, this research addresses a "knowledge void" research gap (Müller-Bloch/Kranz 2015). The final coding is summarized in a table (see Table 3 in the Appendix B).

4.3 Theoretical Background

4.3.1 Assurance about Partners' Intentions

Assurance is defined "as an expectation of benign behavior for reasons other than goodwill of the partner" (Yamagishi/Yamagishi 1994). Therefore, assurance is based on the knowledge of the incentive structure surrounding the relationship of two parties (Yamagishi/Yamagishi 1994). Such knowledge is particularly important in situations with high environmental uncertainty in which an actor does not have the capability of correctly detecting the partner's intentions (Rindfleisch/Heide 1997).

To gain knowledge of the incentive structure surrounding a (potential) relationship, individuals seek sources which provide additional information about (potential) partners (Williams 1997). These sources either accumulate information sufficient for allowing to be certain about (potential) partner's intentions, provide deterrence against unilateral defection, or induce the partner to take a certain course of action with the use of strategies such as "tit-for-tat" (Yamagishi/Yamagishi 1994; Axelrod/Hamilton 1981; Shapiro et al. 1992). Each source increase predictability in interactions or expectations within (potential) exchange relationships for reasons other than only the goodwill of the partner.

4.3.2 A Psychological Perspective of Control as a Source of Assurance

Research on assurance which considers the knowledge about the incentive structure surrounding (potential) relationships is based on a control agency perspective. In particular, this perspective allows not only an examination of the effects of personal control in which the individual acts as an assurance agent to protect information, but also includes proxy control and collective control (Xu et al. 2012b; Yamaguchi 2001). In proxy control, powerful others (such as the government and industry regulators) act as the assurance agents (Xu et al. 2012b; Yamaguchi 2001). In collective control, a collective acts as the assurance agent (Yamaguchi 2001).

The personal control approach aims to directly assure outcomes from a client's perspective. People experience greater autonomy when they exercise direct personal control as the assurance agent (Yamaguchi 2001; Johnston/Warkentin 2010; Xu et al. 2012b). Such control empowers individuals with mutual control over how their data and information, for example, may be used by service providers via technological and non-technological self-protection approaches (Xu et al. 2012b; Yamagishi/Yamagishi 1994). By using personal control, actors induce the partner to take a certain course of action with the use of strategies such as "tit-for-tat" (Axelrod/Hamilton 1981; Wang et al. 2008; Xu et al. 2011). Using these strategies, actors match their own behaviors to those displayed by personal control mechanisms (e.g. cooperating or trustful versus competing or opportunistic) (Axelrod/Hamilton 1981).

The proxy control approach aims to indirectly assure outcomes via powerful others (Son/Kim 2008; Hui et al. 2007; Tang et al. 2008). Institutional mechanisms are used from partners with few resources or low power to gain assurance through skillful and powerful third parties (e.g. industry self-control or legislation) (Bandura 2001; Yamaguchi 2001). These mechanisms enable partners to access resources from third parties, such as knowledge and power, to assure outcomes. In case of opportunistic behavior, these assurance structure provide mechanisms of voice and recourse for the betrayed, which could create strong incentives for firms to refrain from opportunistic behavior and behave appropriately (Benassi 1999; Xu et al. 2011; Shapiro et al. 1992).

In the collective control approach, an individual, as a member of a group or collective that serve as an assurance agent, attempts to control the environment or outsiders. In collective control, responsibility, as well as agency, will be diffused among actors (Latané/Darley 1970). In the collective control approach, individuals attempt to share responsibilities among actors, internalize reference groups, and use their collective knowledge for decision making (Venkatesh et al. 2003; Yamaguchi 2001). Therefore, the collective is responsible for possible positive and negative outcomes to the same extent (Yamaguchi 2001).

4.4 Findings

We adopted a psychological perspective of control and developed a theoretical framework for RAMs, its antecedents, and effects to provide a comprehensive overview and conceptual consensus for RAMs.

Therefore, the theoretical framework (Figure 4) posits that three sets of RAMs – personal control, proxy control, and collective control – influence individuals' beliefs, intentions, and behaviors when concerns are in place.

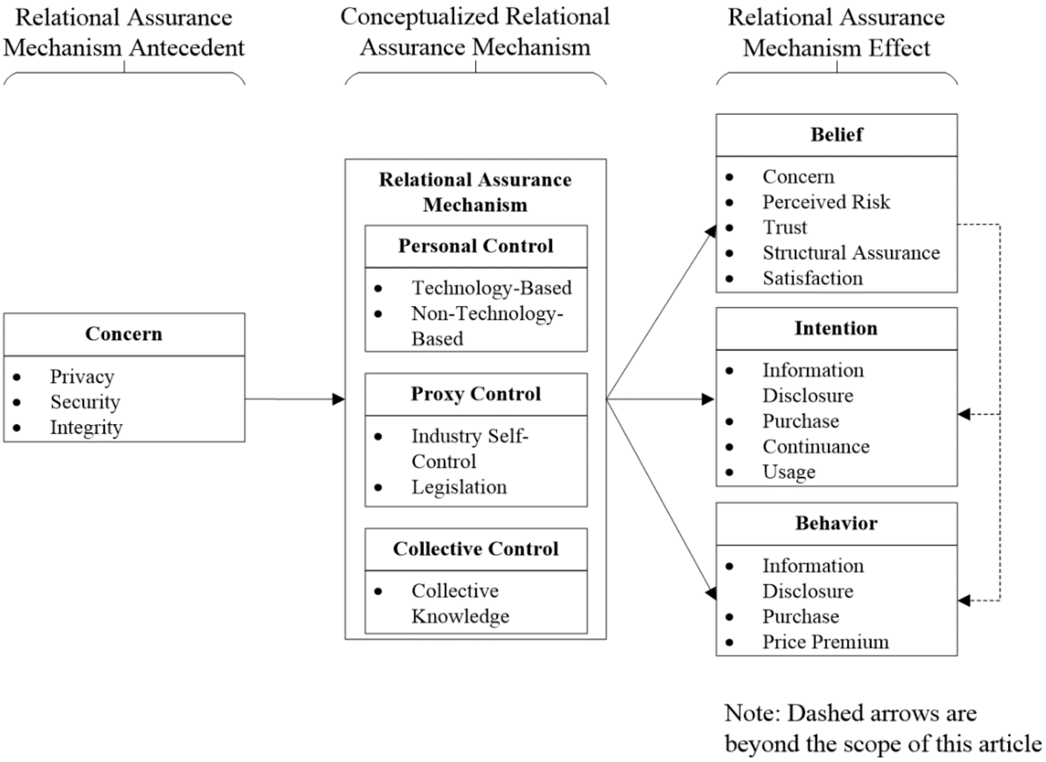


Figure 4. Theoretical Framework for Relational Assurance Mechanisms

Within the following sections, we outline the conceptualization of RAM, its antecedents, and effects in detail.

4.4.1 Conceptualization of Relational Assurance Mechanism

RAMs provide information about the incentive structure of (potential) partners and therefore, increase predictability in interactions or expectations within (potential) exchange relationships. According this notion, Table 8 summarizes the identified examples of RAMs using the key term "assurance" from our literature review. To distinguish the different examples of RAMs we provide a clear definition for each.

Example	Definition	Source
Certification	Defines an endorsement from a third-party organization attesting that a (potential) partner adheres to the organization's policy and a set of standards.	(McKnight et al. 2002a)
Corporative norm	Cooperative norms are defined as the values, standards, and principles to which a population of organizations adheres.	(Pavlou 2002)
Feedback mechanism	Feedback mechanisms accumulate and disseminate information about the past trading behavior of organizations.	(Pavlou 2002)
Law	Mandatory legal rules to ensure adequate protection of information.	(Xu et al. 2012b)
Monitoring	A set of activities undertaken to assure that all transactions are performed as specified by a predetermined set of widely accepted agreements and rules.	(Pavlou 2002)
Persona-lization	Former mechanism which comprises tools and approaches that enable individuals to directly control outcomes.	(Xu et al. 2012b)
Product description	The extent to which a consumer believes that a website is helpful in terms of fully evaluating a product.	(Dimoka et al. 2012)
Redundancy	The inclusion of extra components, which are not strictly necessary to functioning, in case of failure of other components.	(Burt 2009)
Recommen-dation	A suggestion or proposal as to the best course of action.	(Xiao/Benbasat 2007)
Reputation	Reputation is imperfect and indirect information about a potential partner's traits.	(Yamagishi/Yamagishi 1994)
Site quality	Reflects consumers' overall perceptions of how well they think a site works and looks, particularly in comparison to other sites.	(Lowry et al. 2008)
Social Influence	Individual perceives support in decision making from his or her colleagues and others whose opinions matter.	(Venkatesh et al. 2003)
Standardi-zation	The extent to which rules, procedures, and standards exist to guide the conduct of an activity and to evaluate performance.	(Aubert et al. 2012)
Statement	A statement supplied by a (potential) partner that provides argumentation and claims to address certain concerns (e.g. privacy concerns).	(Kim/Benbasat 2009)
Warranty	A warranty signals service quality and provides consumers some assurance in case of service failure.	(Purohit/Srivastava 2001)

Table 8. Identified Relational Assurance Mechanism Examples and their Definitions

Drawing on the work of Yamaguchi (2001) on the differentiation of assurance agent perspectives, we conceptualize RAMs using the assurance agent perspectives personal control, proxy control, and collective control and highlight prominent paper examples.

Within personal control, individuals strive for primary control over their environment. For this assurance agent, literature suggest two major types of RAMs: technology-based and non-technology-based approaches (Son/Kim 2008). Technology-based approaches include features such as monitoring, personalization, or technology redundancy (e.g. (Keith et al. 2015; Johnston/Warkentin 2010)). Non-technological-based approaches are reading corporative norms, product descriptions or statements, providing direct feedback, considering existing warranties, site-quality, or standardization practices (e.g. (Keith et al. 2015)).

Proxy control describes institutional-based assurance of control whereby powerful forces act as the assurance agents. According to literature, individuals particularly rely on industry self-regulation and legislation to exercise proxy control (Xu et al. 2012b). Our research identified the use of specific certifications and laws as examples of industry self-regulation and legislation RAMs (e.g. (Xu et al. 2012b)).

In collective control, one attempts to control the environment or outsiders as a member of a group or collective, which serves as an assurance agent. According to Yamaguchi (2001), individuals "believe they are more efficacious as a collective than as an individual person". Therefore, individuals use their collective knowledge as a RAM to indirectly control the environment or outsiders. While reputation provides assurance for committed individuals to deal with uncertainty when involved with outsiders, social influence refers to an "individual's internalization of the reference group's subjective culture, and specific interpersonal agreements that the individual has made with others, in specific social situations" (Yamagishi/Yamagishi 1994; Venkatesh et al. 2003) (e.g. (McKnight et al. 2002a)). Furthermore, by using the collective knowledge provided from internal or external sources, such as recommendations or reviews via feedback mechanisms, individuals overcome their concerns and adopt or continue a relationship (Keith et al. 2010; Keith et al. 2015) (e.g. (Bansal et al. 2015)).

Based on the assurance agent perspective, Table 9 summarizes our conceptualization of RAMs and identifies examples of these mechanisms from our literature review.

Assurance Agent	**Relational Assurance Mechanism**	**Identified Examples**
Personal Control	Technology-Based	Monitoring, Personalization, Redundancy
	Non-Technology Based	Corporative Norm, Product Description, Site-Quality, Feedback Mechanism, Standardization, Statement, Warranty
Proxy Control	Industry Self-Regulation	Certification
	Legislation	Law
Collective Control	Collective Knowledge	Reputation, Social Influence, Recommendation, Feedback Mechanism

Table 9. Conceptualization of Relational Assurance Mechanisms

In order to gain insights about how RAM concepts are interrelated, we next discuss the antecedents of RAMs as identified in literature.

4.4.2 Concerns as Antecedents of Relational Assurance Mechanisms

Based on the selected literature, we were able to identify three types of concerns that rise an individual's need for RAMs: privacy concerns, security concerns, and business integrity concerns. In the following section, we briefly explain each concern.

Privacy concerns are a primary concern dimension within IS literature, particularly in online transactions (Bansal et al. 2015; Hui et al. 2007; Keith et al. 2015; Kim et al. 2015; Xu et al. 2012b). Privacy concerns within an online context are defined as individuals' concerns about the threat to their information privacy when submitting their personal information on the internet (Keith et al. 2015; Bansal et al. 2015). Studies have identified that as privacy concerns increase, individuals seek RAMs (Oezpolat et al. 2013; Bansal et al. 2015); contrastingly, RAMs will lead to lower privacy concerns (Kim et al. 2015; Xu et al. 2012b). Hence, privacy concerns and the presence of RAMs are highly negatively correlated.

Another antecedent of assurance identified in our review are *security concerns* (Johnston/Warkentin 2010; Keith et al. 2015; Kim et al. 2015; Sun et al. 2006). Based on the dimensions provided by Kim et al. (2004), we distinguish between three types of security concerns: general security issues, transaction integrity, and authenticity of parties to transact. General security issues consist of insider abuse, unauthorized access, distributed denial of service attacks, and malware (Johnston/Warkentin 2010; Keith et al. 2015; Pavlou 2002). Transaction integrity is based on deletion, duplication, or alteration of documents (Kim et al. 2015; Srivastava/Mock 1999b). Alteration of documents refers to identity theft or authentication issues (Khazanchi/Sutton 2001). Security concerns depend not only on the security level of a firm, but also on the knowledge of individuals: e.g., how effective does the individual perceive the security protection mechanisms to be (Kim et al. 2015; Kim 2008).

Business integrity concerns are almost neglected within IS research even if such concerns have been identified as highly significant inhibitors for adoption decisions (Kim et al. 2015). Such concerns are related to how (potential) partners (re-)use collected information from their customers and the possibility that a person or company may not fulfil a promise or complete a task. Especially within high environmental uncertainty, such concerns occur as a result of information asymmetry between (potential) exchange partners (Keith et al. 2015). Such concerns may be amplified by the exponential proliferation of online scams and fake websites (Kim et al. 2004).

In the following section we outline the effects of RAMs on individuals as presented in our literature set.

4.4.3 Effects of Relational Assurance Mechanisms

This section outlines the effects of RAMs on an individual’s beliefs (concern, perceived risk, trust, structural assurance, and satisfaction), intentions (information disclosure, purchase, continuance, and usage), and behaviors (information disclosure, purchase, price premiums).

First, RAMs affect an individual’s *beliefs*. As discussed above, RAMs are in place to address certain concerns and therefore, researchers have also examined the effects of RAMs on concerns itself. RAMs, such as laws, certifications, and statements, have negative effects on an individual’s concerns (Hui et al. 2007; Xu et al. 2012b; Xu et al. 2011). According to Xu et al. (2011), concerns are partly mediated by the individual’s perceived sense of control or perceived risk. Furthermore, related to concerns, studies identified the negative effect of product description, site quality, and certification on an indivudal’s perceived uncertainty and perceived privacy risk (Xu et al. 2011; Dimoka et al. 2012; Pavlou et al. 2006). Contrary to these negative effects, positive effects from RAMs, like certification or statements on trust, have been investigated (Keith et al. 2015; Kim/Benbasat 2009, 2006). Studies point out the positive effects of RAMs on structural assurance beliefs. Structural assurance is defined as the belief that success is likely because contextual conditions, such as statements, certifications and warranties, are in place (McKnight et al. 1998). Hence, structural assurance represents the perceived effectiveness of RAMs which are in place (Mousavizadeh/Kim 2015). Lastly, researchers identified positive effects of perceived monitoring, perceived feedback, and cooperative norms on individual satisfaction with services or products (Pavlou 2002).

Second, RAMs affect an individual's *intentions*. All of our identified studies on individuals' intentions considered trusting beliefs as mediators. Such studies point out the positive effects of RAMs, such as statements and site quality, on an individual's intention to disclose information (Bansal et al. 2015; McKnight et al. 2002b). Furthermore, researchers identified positive effects of RAMs on purchase intentions (Kim et al. 2015; Keith et al. 2015), intention to continue the relationship (Pavlou 2002) or intention to use a web site (McKnight et al. 2002b). Since, individuals tend to avoid losses, future research may consider control or risk perceptions as mediators to better explain an individual's intentions (Kahneman/Tversky 1979; Wiesche et al. 2015).

Third, RAMs affect an individual's *behavior*. Studies identified the positive effects of privacy statements, certification, and customization on actual information disclosure (Keith et al. 2015; Hui et al. 2007) and Oezpolat et al. (2013) identified the positive effects of certifications on purchasing behavior. Dimoka et al. (2012) identified that product description and certification positivly influence the behavior to pay price premiums. Since the actual behavior can differ from an indiviudal's beliefs and intentions, further research is needed on how RAMs affect an indivudal's behavior (Sheeran 2002).

4.5 Conclusion

This research was motivated by a fragmented body of knowledge, in which recent investigations largely examined assurance independently from the mechanisms and the concept itself. Based on this fragmented research, a conceptual consensus for RAMs is missing, even if RAMs are an important element of relational governance. To address these gaps, we conducted a systematic literature review, and identified examples of RAMs, as reported in IS literature. Based on this comprehensive overview, our subsequent analysis provides a conceptualization of RAMs. Last, our theoretical framework of RAMs further provides insights about antecedents and effects resulting from RAMs.

Before we conclude our major contributions, certain limitations should be considered when interpreting the results. Our literature review focused on RAMs as an important element of relational governance (Noordewier et al. 1990; Dyer 1997; Gundlach/Cannon 2010). We recognize there are other forms of relational governance mechanisms such as joint actions or trust. While our theoretical arguments should extend to the instantiations of these other mechanisms of relational governance, more empirical work is needed to increase predictability in interactions or expectations within (potential) exchange relationships. Further investigations should particular build on the work of Yamagishi/Yamagishi (1994), who distinguish between trust and assurance by taking social uncertainty into account. They claim, assurance is particular important in situations with low social uncertainty, while trust is needed when social uncertainty is high (Yamagishi/Yamagishi 1994). Another possible area of interest is to consider the influence of RAMs over time. Prior studies already found changes in the relevance of uncertainty for formal governance mechanisms (Pflügler et al. 2015; Schermann et al. 2016).

Our main contribution to the conceptualization framework of RAMs is threefold. First, we provide insights of the interrelation of existing assurance research and offer insights into how RAMs can be conceptualized. Second, we provide a theoretical framework to consider the concepts of RAMs and how these concepts are related to the antecedents and effects of RAMs. Third, we contribute to practice by providing an overview of existing RAMs and their effects (Lang et al. 2016). Such findings might be used by practitioners, like security managers or auditing authorities, in order to adopt effective RAMs to increase predictability in interactions within exchange relationships.

4.6 Acknowledgements

This research was funded by the German Federal Ministry for Education and Research (grant. No. 16KIS0078).

5 Comparing ITO and Cloud Service Provider Selection Criteria

Title	What Are the Most Important Criteria for Cloud Service Provider Selection? A Delphi Study
Authors	Lang, Michael* (michael.lang@in.tum.de) Wiesche, Manuel* (wiesche@in.tum.de) Krcmar, Helmut* (krcmar@in.tum.de) *Technische Universität München, Chair for Information Systems, Boltzmannstraße 3, 85748 Garching, Germany
Publication	European Conference on Information Systems (ECIS)
Status	Accepted
Contribution of First Author	Problem Definition, Research Design, Data Analysis, Interpretation, Reporting

Table 10. Fact Sheet Publication P2

Abstract

Selecting an appropriate cloud service provider (CSP) is one of the most important challenges affecting sourcing performance. Although cloud computing (CC) relies on the principle of information technology outsourcing (ITO), it remains unclear if selection criteria for ITO provider hold true. Hence, the purpose of this research is to identify the most important criteria for the selection of cloud service providers (CSP). We do this by conducting a Delphi study which includes 16 cloud service decision makers across different cloud service models, company sizes, and industry types. Our results show consensus on CSP selection criteria and identify functionality, legal compliance, contract, geolocation of servers, and flexibility as top five CSP selection criteria. From a theoretical perspective, we demonstrate that results from ITO research hold true for CC research as differences in delivery model and arrangement between ITO and CC will be considered. Practitioners like CSP and cloud decision makers get guidance from our findings to conduct optimal cloud service investments. This is the first study which provides a comprehensive view on relevant criteria for CSP selection.

5.1 Introduction

The worldwide spending on Cloud Computing (CC) is expected to grow 15.7% to $176 billion in 2015 (Gartner 2015). For 2018, various industry reports predict that the majority of global information technology (IT) spending will be related to CC (Galer 2015). In contrast to in-house IT solutions, CC is by definition "a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources […] that can be rapidly provisioned and released […]" (Mell/Grance 2011)[1]. Therefore, CC promises lower cost, increasing productivity and IT elasticity advantages, and enables new business models and values for cloud customers as well as cloud service providers (CSP) (Morgan/Conboy 2013). To benefit from this development, a growing number of companies have entered the CC market by providing distinct cloud services (Kourtesis et al. 2014; Menzel et al. 2015). Prominent examples are Amazon, Google, Microsoft, Rackspace, and GoGrid who are providers of infrastructure as a service (IaaS) and platform as a service (PaaS). SalesForce, Cisco WebEx and DATEV are well-known providers of software as a service (SaaS). Hence, in today's digital age, CC has become an ubiquitous and important technology paradigm (Gupta et al. 2013).

Overall, from a customer's point of view, CC can be seen as an evolution and specific form of information technology outsourcing (ITO) and shares basic principles and benefits with ITO (Chen/Wu 2013). CC customers leverage CSP expertise and infrastructure to run a business which in turn relies on the principle of ITO (Chen/Wu 2013). Furthermore, CC and ITO share basic benefits such as cost savings, access to specialized resources, and the enabled flexibility to respond quickly to market changes (Schneider/Sunyaev 2016; Leimeister et al. 2010; Benlian/Hess 2011).

The selection of an appropriate CSP and ITO provider is one of the most important challenges affecting sourcing performance (Chang et al. 2012; Garrison et al. 2012; Garrison et al. 2015; Jain/Thietart 2013). E. g., productivity and performance advantages within an ITO relationship are only possible if the right provider is selected (Chang et al. 2012). Professional skills, capacity of services, capacity of operation, and external evaluation have been identified as the most important criteria influencing ITO provider selection decisions (Chang et al. 2012). Because CC is highly related to ITO, the extensive body of research on ITO provides a valuable basis for investigating CSP selection decisions.

While CC is a technology-enabled arrangement where customers tend to short-term relationships, ITO is an (human) asset specific arrangement where customers tend to long-term relationships (Chen/Wu 2013). Therefore, CC can be better described as a market-based outsourcing arrangement while ITO as a hierarchical outsourcing arrangement (Gurbaxani/Whang 1991; Chen/Wu 2013). Comparing to hierarchical outsourcing arrangements, within market-based arrangements the customer faces operational (transactional) and contractual (writing contracts) costs (Gurbaxani/Whang 1991; Xin/Levina 2008). As such

[1] While public cloud services are available from a third party provider via Internet and are very cost effective way to deploy information technology solution, private cloud services are managed within an organization and have a strong resemblance to the traditional on premise service type. Therefore, this article focus on public cloud services.

differences between CC and ITO exist, it is unclear if ITO provider selection criteria also hold true for selecting CSP.

Prior qualitative research on CSP selection decisions deductively identified up to 21 criteria affecting selection decisions (Kaisler et al. 2012; Repschlaeger et al. 2012; Repschläger et al. 2011). Quantitative research identified the importance of security and privacy criteria for CSP selection decisions and the relevance of specific criteria for selection decisions within hierarchical groups including IT security and compliance (Gupta et al. 2013; Lübbecke/Lackes 2015; Repschlaeger et al. 2013). Nevertheless, research does not provide a comprehensive view on relevant functional and non-functional CSP selection criteria as experienced by CC decision makers.

From a practical point of view, with the increasing amount of CSP, efficient and accurate provider discovery and selection is a significant challenge for decision makers (Luftman et al. 2015; Sun et al. 2014; Yang/Tate 2012). Cloud decision makers need to consider functional and non-functional criteria across a variety of CSP to select the right one (Garg et al. 2013). Since information transaction in market-based relationships is costly (Gurbaxani/Whang 1991), decision makers need to focus on most important criteria (Luftman et al. 2015; Sun et al. 2014; Yang/Tate 2012).

In order to address the lack of research on CSP selection decisions, we conducted an exploratory study of experts' opinions – a Delphi study. Our study compiled the knowledge of 16 experts using a three-phase process to identify, select and rank CSP selection criteria. Using a Delphi study design, we aim to address the following research question: *What are the most important criteria, as identified by experts, for the selection of cloud service providers?* Our study findings not only contribute to extending the understanding of CC and its relationship to ITO, but also provide valuable insights to enable professionals to make optimal cloud service decisions (Garrison et al. 2012; Garrison et al. 2015).

The remainder of the paper is organized as follows. First, we present the theoretical background for our study by describing the current state of research on ITO provider selection and CC as a specific form of ITO. Further, we point out the decision makers' challenges for CSP selection shaped by an increasing amount of CSP. We then explain our methodological approach and describe the three-phase Delphi study applied in our research. In the findings section, we present a list of ranked CSP selection criteria. Finally, we discuss our results from which we derive implications for future research and practice.

5.2 Research Background

5.2.1 IT Outsourcing Provider Selection

The selection of an appropriate ITO provider is one of the most important challenges affecting sourcing performance (Chang et al. 2012; Jain/Thietart 2013). ITO is a phenomenon in which a customer transfers property or decision rights using IT infrastructure to a provider's organization (Loh/Venkatraman 1992; Chen/Wu 2013). Previous literature on ITO has looked at determinants of outsourcing success (Jain/Thietart 2013; Agrawal et al. 2006; Lacity et al.

2010) and particularly on ITO selection criteria (Chang et al. 2012; Liang et al. 2015; Michell/Fitzgerald 1997). *Table 11* presents an overview of prior research on ITO provider selection criteria.

ITO Provider Selection criteria	**Description based on Chang et al. (2012))**	**Sources**
Professional capabilities and skills	Current technique and prospective developmental capacity of ITO provider companies.	(Liang et al. 2015; Michell/Fitzgerald 1997; Tiwana/Bush 2007; Jain/Thietart 2013; Kourtesis et al. 2014; Chang et al. 2012)
Capacity of services	ITO provider companies after-sales service, and degree of description of products.	(Liang et al. 2015; Tiwana/Bush 2007; Chang et al. 2012)
Capacity of operation	Internal operations and management, and stability of ITO provider companies	(Jain/Thietart 2013; Michell/Fitzgerald 1997; Chang et al. 2012)
External evaluation	ITO provider companies' knowledge on client's industry and their locations.	(Michell/Fitzgerald 1997; Tiwana/Bush 2007; Chang et al. 2012)

Table 11. IT outsourcing provider selection criteria as reported in IS literature

As described in *Table 11*, prior research identified providers' professional capabilities and skills, capacity of services, capacity of operation, and external evaluation as criteria for ITO provider selection (Chang et al. 2012). Hence, ITO customers select providers who are able to add value to existing in-house capabilities and skills (Liang et al. 2015; Michell/Fitzgerald 1997; Tiwana/Bush 2007; Jain/Thietart 2013). According to Michell/Fitzgerald (1997)), the provider should be able to explore new solutions instead of simply reproducing existing ones. Furthermore, ITO customers select providers who offer proper services and operations (Liang et al. 2015; Tiwana/Bush 2007; Chang et al. 2012). Hence, service models, contractual arrangements, and the provider's colocation are vital aspects for provider selection (Jain/Thietart 2013; Michell/Fitzgerald 1997). Finally, ITO decision makers consider external evaluation criteria, such as the provider's reputation or knowledge of the customer's industry, when making provider selection (Michell/Fitzgerald 1997; Tiwana/Bush 2007; Chang et al. 2012). ITO provider selection is therefore well examined and provides a valuable basis for investigating CSP selection decisions.

5.2.2 Cloud Computing as a Specific Form of IT Outsourcing

According to Chen/Wu (2013), from a customer's point of view CC can be seen as an evolutionary development and specific form of ITO and they share basic principles, benefits, and challenges. First, CC customers leverage the provider's expertise and infrastructure to run a business which in turn relies on the principle of ITO (Chen/Wu 2013). Second, both CC and ITO benefit from cost savings, access to specialized resources, and the enabled flexibility to respond quickly to market changes (Schneider/Sunyaev 2016; Leimeister et al. 2010; Benlian/Hess 2011). Third, CC and ITO customers are challenged to select optimal provider to ensure ex-post sourcing performance (Garrison et al. 2012; Jain/Thietart 2013; Agrawal et al. 2006). Therefore, we argue that the extensive literature on ITO is relevant also for research on the determinant criteria of CC (Chen/Wu 2013; Schneider/Sunyaev 2016).

However, even if CC is an evolutionary development of ITO, different characteristics between ITO and CC exist and therefore CC has to be considered as a specific form of ITO. *Table 12* illustrates characteristics of ITO and CC within certain dimensions: *delivery model, scope, contract, and arrangement*. CC is technology-enabled outsourcing via the internet *(delivery model*), based on standard interfaces and functionalities (*scope*) that are available to all user firms (*delivery model*) (Chen/Wu 2013; Mell/Grance 2011). Traditional outsourcing, on the other hand, often entails the transfer of human and physical assets (*delivery model*) and services are customer-tailored (*scope*) and available to dedicated firms (*delivery model*) (Xin/Levina 2008; Susarla et al. 2003; Linstone/Turoff 1975; Chen/Wu 2013). As a result, traditional outsourcing usually involves long-term contracts while CC involves flexible short-term contracts with consumption-based pricing models (*contract*) (Schneider/Sunyaev 2016; Benlian/Hess 2011; Dongus et al. 2014). Hence, CC arrangements are best described as market-based arrangements, while traditional outsourcing arrangements are best described as hierarchical arrangements (*arrangement*) (Gurbaxani/Whang 1991; Chen/Wu 2013).

Based on these characteristics, CC has to be considered as a specific form of ITO and different outcomes from evolutionary development results (see *Table 12*). Because CC is technology-enabled and available to all customers' firms IT resources are better described as a commodity good and not as a source of competitive advantage anymore (Chae et al. 2014; Chen/Wu 2013). The standardization of interfaces and functionalities enables customers to adopt cloud services without facing up-front investments (Susarla et al. 2003; Xin/Levina 2008). At the same time, CSP are able to rapidly provide and release cloud services for new customers with minimal management effort (Mell/Grance 2011). The contractual mode of cloud services with short-term contracts enables customers to switch between providers more often if not satisfied with the service (Schneider/Sunyaev 2016; Benlian/Hess 2011; Dongus et al. 2014). Finally, within a market-based arrangement, customer faces operational (transactional) and contractual (writing contracts) costs when selecting CSP (Gurbaxani/Whang 1991; Chen/Wu 2013; Xin/Levina 2008). As such differences between CC and ITO exist, it is unclear if ITO provider selection criteria also hold true for selecting CSP.

Dimension	Characteristics of ITO	Characteristics of CC	Outcomes from evolutionary development of CC	Source
Delivery Model	Often entails transfer of human and physical assets available to dedicated customers' firms	Technology-enabled outsourcing via the internet available to all customers' firms	Commoditization of IT resources leads to equalization of competitive advantages regarding used IT.	(Chen/Wu 2013; Chae et al. 2014)
Scope	Customer-tailored services	Standard interfaces and functionalities	No up-front investments for new customers are necessary for both customer and CSP.	(Xin/Levina 2008; Susarla et al. 2003; Mell/Grance 2011)
Contract	Long-term contracts (fixed or time and material pricing models)	Short-term contracts (consumption-based pricing models)	Enable customers to switch between providers more often if necessary.	(Schneider/Sunyaev 2016; Benlian/Hess 2011; Dongus et al. 2014)
Arrangement	Hierarchical arrangement	Market-based arrangement	Customer faces operational (transactional) and contractual (writing and enforcing contracts) costs when selecting CSP.	(Gurbaxani/Whang 1991; Chen/Wu 2013; Xin/Levina 2008)

Table 12. Outcomes from evolutionary development of cloud computing

5.2.3 Decision Makers' Challenges for Cloud Service Provider Selection

Adopting new technologies, such as cloud services, is a complex phenomenon which includes numerous opportunities and challenges (Luoma/Nyberg 2011). In order to decrease complexity, prior research identified three subsequent problem areas for cloud service adoption: specification, selection, and contract management (Van der Valk/Rozemeijer 2009; Wollersheim/Krcmar 2013). As this research focuses on criteria for CSP selection, we briefly describe the first two problem areas and exclude contract management as this area first becomes important after the selection of a certain provider.

Within the specification and selection area, customers are challenged to identify necessary environmental, organizational, purchase and buying centre characteristics to specify criteria that the cloud service has to satisfy (Wollersheim/Krcmar 2013). Environmental characteristics include legal issues related to certain technologies. Organizational characteristics to be considered include the fit to existing IT architecture and available infrastructure. Depending on the firm's strategy, different risks are acceptable and control mechanisms are needed and will subsequently define purchase characteristics. Finally, buying centre characteristics are defined by buying networks or the composition of the buying centre. Hence, the specification and selection area involves complex criteria decision makers need to consider when selecting CSP.

Prior studies have examined relevant criteria for CSP selection decisions focussing on qualitative, literature based approaches to determine CSP selection criteria (Kaisler et al. 2012; Repschlaeger et al. 2012; Repschläger et al. 2011). Subsequent research selected dedicated items (cost reduction, security and privacy, and reliability) and analysed quantitatively the effects of these items on cloud decisions (Gupta et al. 2013; Lübbecke/Lackes 2015). As an initial result, the researchers identified security and privacy issues as the most important criteria influencing CSP selection decisions. An early approach to analyse different CSP selection criteria quantitatively used an analytic hierarchy process method (Repschlaeger et al. 2013). Because of the complexity of this method, at most seven criteria could be compared concurrently (Repschlaeger et al. 2013). Most studies focused on qualitative and deductive approaches or compared selective criteria which means no comprehensive overview for most important CSP selection criteria as experienced by CC decision makers exists.

The distinctive characteristics of CC and the poor understanding of important CSP selection criteria calls for further research. This research, therefore, extends the ITO literature by considering CC as an evolution and specific form of ITO.

5.3 Research Approach

To address our research question, we needed input from experts with extensive experience in the cloud computing field and therefore selected the Delphi method. After the Delphi method was developed in the 1950s with the objective of reaching consensus among a panel of experts through an iterative process of controlled feedback (Dalkey/Helmer 1963), IS researchers extensively used such method in the recent years (Chang et al. 2012; Schmidt et al. 2001; Schmidt 1997; Singh et al. 2009). The Delphi method is recommended when "the problem does not lend itself to precise analytical techniques but can benefit from subjective judgments on a collective basis" (Linstone/Turoff 1975). Therefore, the Delphi method provides insights from the collective experience and understanding of an expert panel (Schmidt 1997). Since our study focuses on both identifying most important CSP selection criteria and their relative importance as experienced by experts, the Delphi method was an appropriate choice (Schmidt 1997). The Delphi process stops when a reasonable level of consensus or another pre-defined stop-criterion is achieved (Schmidt 1997; Kendall 1977).

5.3.1 Panel Selection

We recruited experts with significant work experience in the field of cloud computing in order to obtain valid and robust results. We located our panel of experts, responsible for decision making in regard to CSP selection at their place of employment, at cloud computing workshops and through a special interest group for cloud computing on a social network website. Additionally, experts practicing in this field and known to the researchers through prior work experience, were also included in the panel. All potential participants were asked pre-defined questions regarding their cloud experience and use of cloud deployment and cloud delivery models. In order to ensure a reliable panel, we excluded novice persons (those with less than one-year cloud experience), private and hybrid cloud users, and cloud service users who use cloud services less frequently than once a day. We screened our experts to make sure that as many types of industries as possible, organizations of all sizes and usage of various types of cloud service models were represented in the sample. An overview of all panel selection criteria is consolidated in *Table 13*.

#	Selection criteria	Description
1	CSP decision maker	Experts need to be CSP decision makers.
2	Non-novice person	Experts need more than one-year of cloud experience.
3	Public cloud user	The organization has to use public cloud services.
4	Frequent CS user	Experts need to use cloud service at least once a day.
5	Diversity of used cloud service models	Our panel must include at least three types of cloud service models (IaaS, PaaS, SaaS).
6	Diversity of organizational sizes	Our panel must include organizations of all sizes (Large-sized organization, Medium-sized organization, Small-sized organization).
7	Diversity of industries	Our panel must include a high diversity of industries.
8	Diversity of organizations	Our panel must include a high diversity of organizations.

Table 13. Panel selection criteria

We invited 32 experts fitting to our selection criteria described above, of whom 19 participated (see *Table 14*) in the first round of the study which results in an effective response rate of 59%; no obvious response bias regarding our selection criteria were observed. Our panel included three cloud service models (IaaS, PaaS, SaaS), small-, medium- and large-sized organizations, and different industries (financial services, manufacturing, software development, railway, media, energy, data analytics, public administration, and wholesale). While some of the panellists were responsible for CSP selection within their company, others served as consultants and were frequently challenged with CSP selection for their customers. As some experts are responsible for different cloud service models, experts might be listed several times. Overall, each expert worked for a different company which ensures a diverse perspective on our research topic. As *Table 14* shows, the profile of the panel indicates considerable CSP selection experience for diversity of service models, industries, and company sizes, thus establishing the credibility of the panel.

Cloud service model	Involved company categories	Involved industries	Experts
IaaS	LO (>250), SO (10-49)	Media, Financial services, IT-Consultant, Public administration, Data analytics, IT service, Railway, Manufacturing, Software development	CEO 2, Consultant (Manager), Consultant (Partner 1), Consultant (Partner 2), Consultant (Senior), Project Manager, Business Intelligence Manager, IT-Manager 3, IT-Manager 5, IT-Manager 6, Project Manager, COO 2
PaaS	LO (>250), SO (10-49)	Financial services, IT-Consultant, IT service, Manufacturing, Software development	CEO 2, Consultant (Manager), Consultant (Partner 1), Consultant (Partner 2), Consultant (Senior), IT-Manager 5, IT-Manager 6, COO 2
SaaS	LO (>250), MO (50-250), SO (10-49)	Energy, Manufacturing, Financial services, Communication, IT-Consultant, Software development, Financial services, Railway, Wholesale	IT-Manager 1, CEO 1, COO 1*, Consultant (Manager), Consultant (Partner 1), Consultant (Partner 2), Consultant (Senior), IT-Manager 2*, IT-Manager 4, Project Manager, CEO 3, CEO 4*

* left study after iteration 1 of round 3.
LO = Large-sized organization; MO = Medium-sized organization; SO = Small-sized organization

Table 14. Panellists' overview

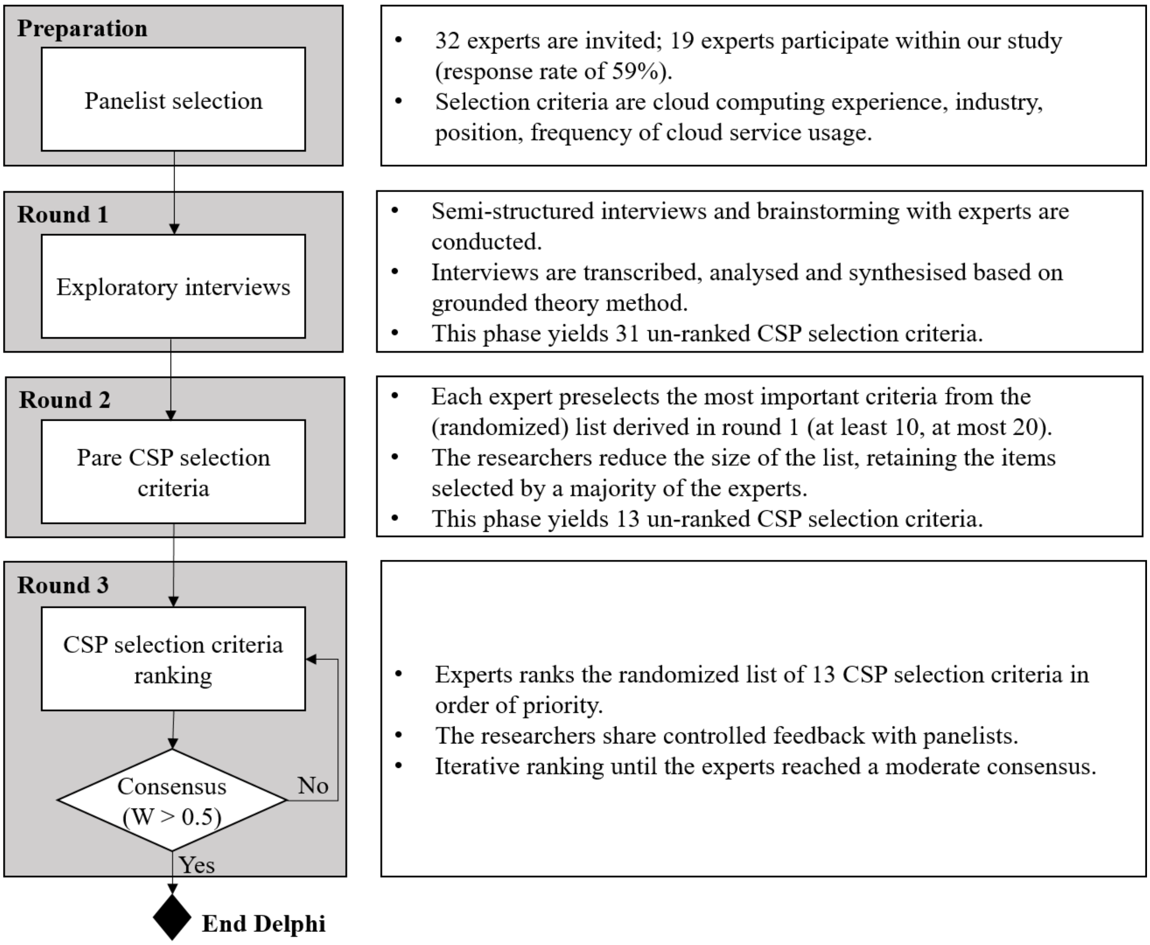
5.3.2 Data Collection and Analysis Method

To investigate the relative importance of CSP selection criteria, we followed a modified version of the Delphi method as proposed by Schmidt (1997). Data was not only collected via brainstorming but also via semi-structured interviews which allowed us to develop a deep understanding of the identified criteria and reasoning behind the participants' individual rankings. Similar to Schmidt et al. (2001) our study design consists of four stages: the preparation stage and three subsequent Delphi rounds (see *Figure 5*). We started our first round in May 2015 and the Delphi study finished in October 2015. Activities during the preparation stage included planning of the study and establishment of the expert panel using a pre-questionnaire as described above.

In round 1, brainstorming and semi-structured interviews with experts were arranged and conducted in order to identify as many CSP selection criteria as possible. While brainstorming enabled us to get a high quantity of possible relevant selection criteria, the semi-structured interviews provided additional information and selection criteria which were not mentioned during brainstorming. After interviewing the experts, the gathered information was transcribed, analysed and synthesised. To aggregate the findings across all interviews, we adapted the method of Strauss/Corbin (1990) and used open and axial coding to identify all relevant criteria. To ensure consistent coding, two researchers independently read and coded all interview transcripts line-by-line using phrases from the transcripts that described CSP selection criteria (open coding) and discussed any conflicting results. This open coding process resulted in a list of 69 codes and 360 phrases. The resulting discussions and the rich body of information within the transcripts provided us with the necessary background information for the subsequent axial coding. After completing the axial coding, we reached a final list of 31 un-ranked CSP selection criteria.

During round 2, we pared the consolidated list of CSP selection criteria into a more manageable set for the ranking phase. Following the suggestion by Schmidt (1997), we presented the experts with a randomised list of the 31 un-ranked CSP selection criteria from round 1 and asked each expert to select (not rank) the most important criteria (at least 10, at most 20) for CSP selection. We provided a brief definition for each selection criterion in order to assure that all experts had the same understanding of each. All 19 experts provided responses in this round 2. After the responses were consolidated, a cut-off value has to be defined which yields to a list of 12 to 15 items for the subsequent ranking phase (Singh et al. 2009). Using this process, we chose a cut-off value of 60% and identified a pared list that included 13 most important CSP selection criteria.

An overview of our overall research process is illustrated in *Figure 5*.



- 32 experts are invited; 19 experts participate within our study (response rate of 59%).
- Selection criteria are cloud computing experience, industry, position, frequency of cloud service usage.

- Semi-structured interviews and brainstorming with experts are conducted.
- Interviews are transcribed, analysed and synthesised based on grounded theory method.
- This phase yields 31 un-ranked CSP selection criteria.

- Each expert preselects the most important criteria from the (randomized) list derived in round 1 (at least 10, at most 20).
- The researchers reduce the size of the list, retaining the items selected by a majority of the experts.
- This phase yields 13 un-ranked CSP selection criteria.

- Experts ranks the randomized list of 13 CSP selection criteria in order of priority.
- The researchers share controlled feedback with panelists.
- Iterative ranking until the experts reached a moderate consensus.

Figure 5. Research process based on Schmidt (1997)

The pared list is transferred to round 3 of the study for ranking. We send the manageable list of 13 CSP selection criteria from the selection round 2 in randomized order to each of our experts and asked them to rank the CSP selection criteria in order of priority. We also asked the experts to explain their reasoning for the chosen ranking. This information would be shared with the experts in subsequent iterations. To measure the degree of consensus among our experts, we followed the approach of Schmidt (1997) and used Kendall's coefficient of concordance (W). Kendall's W is frequently used in Delphi studies and is applied to indicate whether a consensus among the panellists has been reached and the relative strength of the consensus (Schmidt 1997). When Kendall's W is greater than 0.7, strong consensus has been reached, values between 0.5 and 0.7 indicate moderate consensus and values less than 0.5 indicate there is little consensus among panellists (Schmidt 1997). 19 experts participated in the first iteration of ranking in round 3 which yielded a Kendall's W value of 0.22 indicating relatively weak consensus.

Following Schmidt (1997) we decided to continue the ranking process until the coefficient of concordance indicated a moderate consensus. Therefore, we conducted two further iterations within round 3. This time, we provided the following additional information to each expert as controlled feedback: (I) the average rank of each criterion, (II) the ranking given by that expert for each criterion at the prior iteration of ranking, and (III) the percentage of experts who ranked that criterion within the top-50%. As a fourth controlled feedback (IV), we provided a summary of all comments made by the experts for each criterion collected within the prior iteration. Similar to Singh et al. (2009), we believed that this additional information would help the experts to consider their own ranking in light of the group's ranking thus providing them the opportunity to adjust their ranking where it made sense to them to do so. 16 experts participated in the second iteration, yielding a Kendall's W of 0.32. The Kendall's W was 0.69 in our third iteration in which 16 experts participated suggesting that a moderate level of consensus had been reached. According to the rankings made by the experts during iteration three, Kendall's W almost doubled. We believe this result may be due to the fact that the experts were able to reflect their own ranking in light of the panel's ranking by considering the controlled feedback of two iterations. This additional information most likely helped the experts to reach a group consensus.

5.4 Results

Results of our Delphi study are described next. As mentioned, round 1 (exploratory interviews) yielded to 31 un-ranked CSP selection criteria which have been pared to a manageable number of 13 criteria in round 2 (pare) by majority ranking. Results of round 2 are listed and briefly described in *Table 15*.

CSP selection criteria	**Description provided by panel**
Certification	A CSP is certified by an independent authority in accordance with established requirements or standards.
Contract	The provider offers understandable contractual arrangements including a clear cost structure (e.g. consumption-based pricing model).
Control	A CSP provides remote access tools to provide proactive control of data, functionalities and processes (e.g. customization).
Deployment model	A clearly defined deployment model in terms of ownership, control of architectural design, and degree of available customization exists (e.g. private cloud, hybrid cloud, community cloud, public cloud).
Flexibility	A customer can independently adjust the obtained capabilities and the adjustments are carried out automatically within a short period of time and with transparent costs.
Functionality	The set of functions or capabilities (e.g. availability, usability, security, performance requirements) associated with the cloud solution match the demand of the customer.
Geolocation of servers	Geographical location of providers' servers is suitable in terms of data protection legislation and user latency.
Integration	Configuration of the service enables its smooth integration into the IT landscape of the business.
Legal compliance	Due to its geographical location, policies, etc., a CSP complies with legal and regulatory requirements of the customer.
Monitoring	A manual or automated IT monitoring and management technique which provides transparency of cloud service quality.
Support	A CSP possesses a responsive service support, which provides all operative processes necessary for the handling of service interruptions and for implementation of changes.
Test of solution	A CSP enables convenient trial periods of a service.
Transparency of activities	Transparency of security, data privacy, data access, cloud architecture, service level competencies etc.

Table 15. List of 13 un-ranked CSP selection criteria

Within the subsequent round 3 (ranking) the CSP selection criteria were ranked with regard to their relative importance. *Table 16* presents the 13 CSP selection criteria most often identified by the experts, their average rank, the Kendall’s W value for each ranking iteration (round 3), and the final ranking of the selection criteria.

CSP selection criteria	**Iteration 1 average rank**	**Iteration 2 average rank**	**Iteration 3 average rank**	**Final rank**
Functionality	2.95	2.6	1.56	1
Legal compliance	4.79	4.53	2.56	2
Contract	6.42	5.20	3.94	3
Geolocation of servers	5.42	5.27	4.25	4
Flexibility	6.11	6.40	5.75	5
Integration	7.26	7.40	6.88	6
Transparency of activities	7.21	7.07	7.44	7
Certification	8.21	7.20	8.19	8
Monitoring	8.42	8.27	8.75	9
Support	7.89	8.20	9.00	10
Control	8.21	8.67	9.25	11
Deployment model	8.79	9.67	11.56	12
Test of solution	9.32	10.53	11.88	13
Kendall's W*	**0.22**	**0.32**	**0.69**	
* Kendall's W > 0.7 → strong consensus among panellists 0.5 ≤ Kendall's W ≤ 0.7 → moderate consensus among panellists Kendall's W < 0.5 → little consensus among panellists				

Table 16. Intermediate and final ranking of the most important criteria for selecting a cloud service provider

As mentioned, iteration 3 yielded a Kendall's W of 0.69 which indicates that our pre-defined stop-criterion of a moderate consensus was achieved. Since our panel of experts was highly diverse in regard to cloud service model, size of company, and type of industry represented, we conclude that a reasonable degree of confidence in the ranking is reached (Schmidt 1997).

5.5 Discussion

The conduction of this research was motivated by a poor understanding of the validity of existing ITO provider selection criteria within the context of CC. In order to enhance understanding of this issue, we conducted a Delphi study to identify criteria of importance to experts when selecting CSP. The study yielded the identification and ranking by importance of 13 CSP selection criteria (see *Table 16*).

5.5.1 Relation between Selection Criteria for Cloud Service Provider and IT Outsourcing Provider

The 13 important criteria for selecting cloud service providers, can be used to make optimal CC investment decisions. Because CC can be seen as an evolution and specific form of ITO, as listed in *Table 17*, we are able to conceptually and directly compare our results to the ITO provider selection criteria reported by Chang et al. (2012). As a structure for our discussion, we use the identified ITO provider selection criteria "capacity of professional skills", "capacity of operation", "capacity of service", and "external evaluation" from Chang et al. (2012).

Chang et al. (2012) defined capacity of professional skills as a current technique and prospective developmental capacity of ITO companies. According to this definition, capacity of professional skills can be connected conceptually to *functionality*, *flexibility*, and *integration* (see *Table 17*) (Lankton et al. 2014). For example, while an ITO provider can perform tasks well, provide flexible problem solving, and make good decisions for future developments, a cloud service cannot perform all these tasks. A cloud service can only perform functions or provide and integrate flexible features which the user requires to accomplish a particular task (Lankton et al. 2014). *Functionality*, *flexibility*, and *integration* are important CSP selection criteria as a customer buys and integrates a certain service to solve problems in a flexible way (Mell/Grance 2011).

ITO provider selection criteria	**Evolution and specific form of CSP selection criteria**	**Conceptual or direct link between ITO and CC**
Capacity of professional skills	Functionality	Lankton et al. (2014))
Capacity of operation	Legal compliance	Ang/Cummings (1997))
Capacity of operation	Contract	Tiwana/Bush (2007))
Capacity of operation	Geolocation of servers	Han/Lee (2012))
Capacity of professional skills	Flexibility	Mell/Grance (2011))
Capacity of professional skills	Integration	Mell/Grance (2011))
External evaluation	Transparency of activities	Meiseberg (2015))
External evaluation	Certification	Sunyaev/Schneider (2013))
External evaluation	Monitoring	Meiseberg (2015))
Capacity of services	Support	Han/Lee (2012))
Capacity of operation	Control	Han/Lee (2012))
Capacity of services	Deployment model	Mell/Grance (2011))
Capacity of services	Test of solution	Chang et al. (2012))

Table 17. Evolution and specific form of CSP selection criteria based on Chang et al. (2012)

Capacity of operation can be related to *legal compliance*, *contract*, *geolocation of servers*, and *control*. For example, ITO customers tend to use formal and informal controls such as contractual arrangements, frequent status meetings, or operation-check visits on the ITO provider site (Tiwana/Bush 2007). Since CSP provide their services over the internet, frequent personal status meetings and visits on the CSP site are not always possible. Instead, a CSP can be indirectly controlled by considering the *legal compliance* of the CSP and the *geolocation of servers* (Han/Lee 2012; Ang/Cummings 1997). In order to consider specific requirements regarding service costs or service descriptions, contractual arrangements and provided control mechanisms are relevant criteria for CSP selection (Tiwana/Bush 2007; Han/Lee 2012).

Capacity of services can be directly related to a *support* and *deployment model* and conceptually related to *test of solution*. End-user support as well as the available service model (for ownership) are important for both selection of ITO and cloud service providers (Chang et al. 2012; Mell/Grance 2011). *Test of solutions* are additional services which help to persuade potential customers to use CSP. Since capacity of services describes service related issues (Chang et al. 2012), a conceptual connection to *test of solution* is appropriate.

Finally, external evaluation can be related directly to *transparency of activities*, *certification*, and *monitoring*. For example, ITO customers tend to trust any suggestions and/or recommendations coming from known business partners when selecting ITO providers (Chang et al. 2012). Because *transparency of activities*, *certifications*, and *monitoring* are instruments to establish trust (Meiseberg 2015; Sunyaev/Schneider 2013), these identified CSP selection criteria are also applicable as ITO provider selection criteria.

Our results for CSP selection criteria also represent ITO provider selection criteria for a technology-enabled and market-based outsourcing arrangement (see *Table 17*). According to our findings, the rich body of ITO knowledge is still valid within the context of CC, and CC can be seen as an evolution and specific form of ITO.

5.5.2 Limitations, Implications and Future Research

As with any study, the results of the current study must be interpreted in the context of the limitations and constraints which attend its generalisability, expert selection, and abstraction level of CSP selection criteria. First, the final study results are based on the participation of 16 experts and thus, may not be generalisable to a larger population or prescriptive in nature. Being able to analyse results from a larger group of CC decision makers from other firms or countries, or for other cloud delivery models (such as private cloud) would be advantageous for future studies. Second, our experts were not chosen randomly, and we did not attempt to control for the criticality (in terms of data sensibility) for used cloud services. Hence, future research could address this issue by providing a larger, randomized sample and control for criticality of used cloud services. Third, we considered CSP selection criteria on a high abstraction level. To provide further insights, future research may use our results as a research agenda for investigating CSP selection criteria on a lower abstraction level. Therefore, researchers may focus on functionality aspects e.g. considering customers’ functional preferences for different cloud delivery models, on legal compliance e.g. privacy issues, on contract related aspects e.g. different pay-per-use models, or on impact of geolocation of servers on CSP selection within future investigations.

However, to the best of our knowledge, this is the first study to apply a comprehensive scope of experts from multiple industries, of different organizational sizes, and using different cloud service models to identify most important criteria for CSP selection. The results obtained in our study extend criteria mentioned in previous literature for CSP selection and provide a better understanding about their relative importance (Schneider/Sunyaev 2016; Garrison et al. 2012; Garrison et al. 2015). In that vein, contrary to the suggestion of Schneider/Sunyaev (2016), we identified consensus regarding the importance of relevant criteria across different service models. We explain our findings by considering the abstraction level of relevant CSP selection criteria. Since we aimed to also consider non-functional criteria, we combined functional criteria on a high abstraction level and simultaneously consider further non-functional criteria on a high abstraction level. Therefore, on a high abstraction level, the preferences of our experts resulted in consensus. Our interview analysis suggests that functional selection criteria of SaaS solutions may considerably differ from functional selection criteria of IaaS or PaaS solutions when considering different industries or application areas. Hence, we suggest that future research in the CC context should focus on organizational or environmental characteristics to examine differences within functionality aspects.

Our results indicate that inter-organizational control mechanisms within CC context are vital. In traditional ITO, relational controls are in use to complement formal controls like service-level-agreements (SLA) (Gopal/Koka 2012). Particularly, this is important when high task uncertainty exists (Rustagi et al. 2008). CC faces continuously high uncertainty because cloud services are delivered over the internet from an external CSP which means inherently low controllability (KPMG 2015). In order to complement formal controls, CC decision makers need a greater amount of relational control mechanisms, in comparison to ITO decision makers, as the importance of capacity of operations increases for conceptually related CSP selection criteria (Chang et al. 2012; Gopal/Koka 2012).

Since CC is a technology-enabled and market-based outsourcing arrangement via the internet, particularly IS based control mechanism are needed to assure organizational performance and organizational integrity (Schermann et al. 2012; Chen/Wu 2013). IS based control mechanisms enable organizations to detect or even prevent failures, and to assure outcomes (Wiesche et al. 2012). Therefore, we call for further research to examine inter-organizational IS based control mechanisms to reduce market uncertainty.

Overall, our results support findings from previous ITO studies regarding provider selection criteria. Nevertheless, since diverging developments between CC and ITO exist, researchers should re-examine ITO findings within the context of CC in order to identify new developments.

This study presents valuable insights for practitioners. The list of 13 un-ranked CSP selection criteria validated by 19 experts clearly delineates aspects that should be taken into consideration when making CC investment decisions from both the CSP and customer viewpoint. Furthermore, the ranked list of 13 CSP selection criteria provides a compact list containing the most important criteria in the opinion of our experts. This list could enable practitioners to focus on most important information with the greatest influence on optimal CC investment decisions. CSP, or possibly certification authorities, may use this list to provide most important information to cloud customers. Decision makers can use the list to direct their limited resources toward addressing the most important CSP selection criteria.

5.6 Conclusion

In this study, we investigate the most important criteria, as identified by experts, for the selection of CSP. To answer our research question, we conducted an exploratory Delphi study on experts’ opinion. We identified 13 CSP selection criteria and ranked their importance. We further show that our results for CSP selection criteria represent ITO provider selection criteria for a technology-enabled and market-based outsourcing arrangement.

Our main contribution is threefold. First, our results support prior findings that CC can be seen as an evolution and specific form of ITO and the rich body of ITO knowledge should be leveraged within the context of CC. Second, our results serve as a research agenda for future investigations on CSP selection decisions. Third, we contribute to practice by providing a comprehensive overview of most important CSP selection criteria when making CC investment decisions from both the CSP and customer viewpoint.

5.7 Acknowledgement

This research was funded by the German Federal Ministry for Education and Research (grant. No. 16KIS0078). The authors would like to thank the anonymous participants of this Delphi study and Maria Romanenko for supporting the data collection process.

6 Cloud Service Provider Selection Criteria

Title	Criteria for Selecting Cloud Service Providers: A Delphi Study of Quality-of-Service Attributes
Authors	Lang, Michael* (michael.lang@in.tum.de) Wiesche, Manuel* (wiesche@in.tum.de) Krcmar, Helmut* (krcmar@in.tum.de) *Technische Universität München, Chair for Information Systems, Boltzmannstraße 3, 85748 Garching, Germany
Publication	Information & Management (I&M)
Status	Accepted
Contribution of First Author	Problem Definition, Research Design, Data Analysis, Interpretation, Reporting

Table 18. Fact Sheet Publication P3

Abstract

Customers of cloud service providers (CSPs) use different criteria to judge the quality of cloud services. Based on managerial and technical Quality-of-Service (QoS) attributes, these criteria provide information on service quality and the CSP itself. Thus, it is important to identify relevant QoS to assure success of customers. Using a Delphi study, 16 professionals characterized by different cloud service models, company sizes, and industries identified and ranked QoS according to their relative importance. Our results show consensus on QoS. We identify functionality, legal compliance, contract, geolocation of servers, and flexibility as top QoS and observe increasing importance of managerial QoS.

6.1 Introduction

Investments in cloud computing have increased tremendously in the past few years (Woods 2016). As a consequence, many cloud service providers (CSPs) now participate in this competitive market leading to extremely competitive pricing for services (Truong-Huu/Tham 2014; Karunagaran et al. 2016). Not just one, but often several CSPs are able to fulfill basic customer requirements (Garg et al. 2013; Schrödl 2012).

From the cloud customers' point of view, selecting the "right" CSP is essential to assure future performance and maintain compliance with laws, policies, and rules (Garrison et al. 2012; Garrison et al. 2015; Weinhardt et al. 2009; Ragowsky et al. 2014). When using cloud services, cloud customers pool their resources outside of the firm's environment and increase their dependency on networks (Brender/Markov 2013). As a consequence, customers face certain risks such as the risk of information leakage resulting from malicious behavior in shared environments or the risk of service breakdowns because of possible network outages (Subashini/Kavitha 2011). At the same time, an increasing number of laws, policies, and rules forces cloud customers to consider additional requirements such as data protection (Ragowsky et al. 2014; Schneider/Sunyaev 2016). Choosing the wrong CSP can lead to failure in future service delivery, compromised data confidentiality or integrity, and non-compliance with established regulations for use of clouds for data storage (Ghafori/Sarhadi 2013; Whiteside et al. 2012).

To select the "right" CSP, a wide range of technical and managerial Quality-of-Service (QoS) attributes must be considered. For example, technical QoS attributes such as performance or reliability are essential to specify characteristics of the CSP in relation to the cloud service itself and can be measured using specific techniques such as bandwidth or latency tests (Zhou et al. 2007). Technical QoS attributes are fundamental for cloud customers who expect providers to deliver advertised characteristics (Zhou et al. 2007). Transparency, however, is limited within the cloud computing environment, and customers may not have complete information to assure performance and attain or maintain regulatory compliance (Godse/Mulik 2009; Huang/Nicol 2013). Moreover, the technology associated with cloud computing changes quickly and continually because of short technology life-cycles (Lins et al. 2016). To adequately assess and verify the range of technical QoS attributes, cloud customers require managerial QoS. Managerial QoS attributes such as geolocation of servers or monitoring services verify and assure the capabilities and advertised characteristics of a CSP (Tran et al. 2009).

Web services in general (Ran 2003), and particularly cloud services, have extremely diverse QoS attributes for similar characteristics (Ghosh et al. 2015; Petri et al. 2015); the quality of security or performance offerings of cloud services, for example, may be highly variable (Garg et al. 2013). Furthermore, not all technical QoS attributes are directly measurable for cloud customers (Tran et al. 2009) and not all managerial QoS attributes are directly accessible for cloud customers and are difficult to quantify (Zhou et al. 2007). The cloud customer often lacks adequate knowledge to determine which QoS attributes are relevant to meet their needs and which provider can best fulfill their QoS requirements (Huang/Nicol 2013; Ramacher/Mönch 2014).

Research about the most important QoS in CSP selection provides snapshots in 2011 and 2013. While Saripalli/Pingali (2011) provide a list of 25 ranked cloud vendor selection attributes in 2011, Repschlaeger et al. (2013) ranked 62 low-level QoS attributes in 2013. However, legal conflicts related to data protection principles between the United States and Europe increased between 2011 and 2015. Further, the role of information technology (IT) decision makers is evolving from providing and supporting IT toward integrating and retaining IT quality as public cloud computing becomes mainstream (Ragowsky et al. 2014). Hence, the most important QoS attributes may change over time, but our knowledge about the most important QoS attributes that consider environmental changes within the cloud market is limited.

Our work investigates the relative importance of QoS-based selection attributes used by customers within a cloud computing environment in 2015. Using a Delphi study design, we examined the opinions of professionals to achieve consensus on the most important QoS attributes for CSP selection. Our results show consensus on QoS attributes and identify functionality, legal compliance, contract, geolocation of servers, and flexibility as the top five QoS attributes. Through a comparison of our results with previous studies, we identified four key changes that have occurred within the cloud market: (1) an increase in the importance of data protection; (2) cloud customers continue to seek value co-creation with CSP; (3) a decrease in the possibility of CSP opportunistic behavior; and (4) the continuation of product uncertainty as a major problem during CSP selection. From a practical point of view, our results not only provide insights to help cloud customers conduct optimal CSP selection decisions, but these results also help CSP to address cloud customers' needs more effectively through cooperation with independent third parties and the provision of relevant control mechanisms.

The remainder of the paper is organized as follows. First, we present the theoretical background for our study by describing the current state of research on CSP selection processes and QoS attributes. We then explain our methodological approach and describe the three-phase Delphi study applied in our research. In Results, we first present all identified QoS attributes, then the ranking of these attributes provided by the professionals, and a classification of these attributes. Finally, we outline limitations and possible directions for future research and discuss our contribution to literature and practice.

6.2 Research Background

In this section, we first explain the cloud sourcing process in general and define the scope of this study. Then, we point out the state of research on QoS attributes and examine the shortcomings of literature.

6.2.1 Cloud Sourcing Process

Conducting decisions on cloud sourcing is a complex process involving three consecutive steps (Luoma/Nyberg 2011; Zhou et al. 2007; Moe et al. 2017). These steps include the cloud sourcing decision itself, pre-qualification of possible CSPs, and CSP selection (Figure 6).

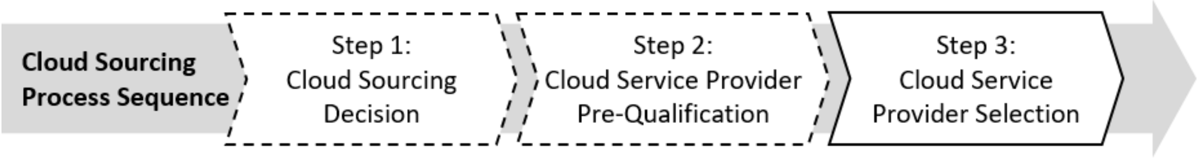

Cloud Sourcing Process Sequence
Step 1: Cloud Sourcing Decision
Step 2: Cloud Service Provider Pre-Qualification
Step 3: Cloud Service Provider Selection

Figure 6. Cloud sourcing process (Step 3 is the focus of this study)

In the first step, cloud customers make a decision on cloud sourcing. Inhibiting and facilitating factors for cloud sourcing affect this decision-making (Benlian/Hess 2011; Oliveira et al. 2014). While an increasing strategic importance of services, available risks, or perceived complexity may prevent cloud customers to cloud source services, the possibility to save costs, access specialized resources, increase flexibility, or reduce time to market facilitates cloud customers to cloud source services (Schneider/Sunyaev 2016; Luoma/Nyberg 2011). Both facilitating and inhibiting factors influence cloud customers to cloud source their services within the initial decision-making step.

In the second step, cloud customers preselect possible CSP depending on functional requirements and boundary restrictions. Only providers that serve required service models (IaaS, PaaS, or SaaS providers) and needed functions or applications (CRM system) are considered (Garg et al. 2013; Schrödl 2012). Boundary restrictions on the data, e.g., sensitive data that are liable to specific regulatory requirements such as accounting systems constitute the list of preselected CSPs (Rieger et al. 2013; Zhou et al. 2007). This list of CSPs might fulfill the purpose of the cloud sourcing endeavor (Garg et al. 2013; Schrödl 2012). The challenge is to discover the “right” CSP that is required by the cloud customer to conduct a detailed CSP examination within the next step (Garrison et al. 2012; Garrison et al. 2015; Weinhardt et al. 2009).

Cloud customers have to select an appropriate CSP, the third step in the decision-making process. Often several CSPs fulfill basic requirements regarding required service model, required functions, or applications (Garg et al. 2013). In addition to functional requirements and boundary restrictions, QoS requirements must be considered (Garg et al. 2013). As an example, CSPs warrant different levels of availability usually varying between 98% and 99.999%. Cloud services have a high diversity of different QoS attributes (Ghosh et al. 2015); cloud customers have to select from a plethora of offerings and decide which QoS attributes are relevant and which provider can fulfill their QoS requirements (Huang/Nicol 2013).

6.2.2 The Challenge to Identify Relevant Quality-of-Service Attributes

Cloud customers base their CSP selection on diverse QoS attributes. QoS attributes describe non-functional aspects of web services (Garg et al. 2013). QoS attributes are used to evaluate the degree to which a web service meets specified technical and managerial quality requirements in a service request (Tran et al. 2009; Zhou et al. 2007). The technical QoS comprises attributes related to operational aspects of web services, such as usability, efficiency, reliability, and performance (Tran et al. 2009). The managerial quality QoS comprises attributes used for capturing service management information such as geolocation of servers or contract (Tran et al. 2009). While technical QoS specifies the CSP characteristics of the cloud service itself, managerial QoS provides a source of decision confidence by verifying the capabilities and advertised characteristics of a CSP (Zhou et al. 2007; Lang et al. 2017, 2018b). To select the right CSP, both technical and managerial QoS attributes must be considered by cloud customers.

Identifying relevant QoS attributes is difficult (Ramacher/Mönch 2014). Web services in general (Ran 2003), and particularly cloud services, have a high diversity of QoS levels for similar functionalities (Ghosh et al. 2015; Petri et al. 2015). Each QoS attribute comprises different meanings. As an example, the performance attributes cover CPU performance, memory performance, and provision time, which highly influence the quality of the underlying infrastructure (El Zant/Gagnaire 2015). Cloud customers also must consider different QoS attributes related to runtime or functional, transaction support, configuration management, and security when selecting CSP (Wang et al. 2015; Ran 2003; Saleem et al. 2015; Wiesche et al. 2015).

Not all attributes of CSP are accessible or can be easily measured (Cayirci et al. 2016). Almost two-thirds of CSPs do not advertise concrete prices to avoid margin cutting price wars (Koehler et al. 2010). Furthermore, the security configuration and capabilities of CSPs are not easy to quantify (Cayirci et al. 2016; Lins et al. 2016). In addition to direct information publicly available from CSPs, cloud customers might also consider indirect information from cloud certificates during CSP selection (Sunyaev/Schneider 2013).

In light of these challenges in identifying relevant QoS attributes, cloud customers may require support in the selection of CSP (Berry et al. 2016).

6.2.3 Approaches to Identify Relevant Quality-of-Service Attributes for Cloud Service Provider Selection

To support cloud customers during CSP selection decisions, Saripalli/Pingali (2011) used a short-list of cloud vendor selection attributes and ranked 25 QoS attributes in 2011. In 2013, Repschlaeger et al. (2013) identified 62 low-level QoS attributes in literature, combined these into 21 QoS attributes and 6 QoS categories, and then ranked the low-level attributes. While Saripalli/Pingali (2011) focus mainly on technical QoS attributes, Repschlaeger et al. (2013) identify a growing number of managerial QoS attributes related to data protection issues. The importance of managerial QoS attributes has increased because cloud technology and the legal environment change rapidly owing to short life-cycles and inherent cloud computing characteristics (Lins et al. 2016; Dove et al. 2015) (Table 19).

Study	Managerial QoS attributes	Technical QoS attributes	Publication date
Saripalli/Pingali (2011)	4 QoS attributes	21 QoS attributes	2011
Repschlaeger et al. (2013)	8 QoS attributes	13 QoS attributes	2013

Table 19. Managerial and technical QoS attributes as identified by Saripalli/Pingali (2011) and Repschlaeger et al. (2013)

However, prior findings are limited because of changes in the legal environment and the changing role of IT decision makers, and they ignore interdependencies between technical and managerial QoS attributes: Cloud customers are challenged to stay compliant with laws, policies, and rules that specify selection requirements. A diversity of different levels for data protection regulation, laws, and rules exist because of a fragmented legal environment relating to data protection (Schneider/Sunyaev 2016; Currie/Seddon 2014). Legal conflicts between the United States and Europe in data protection principles increased between 2011 and 2015 (Dove et al. 2015). One result of this conflict resulted in invalidation of the Safe Harbor Agreement between the United States and Europe in 2015. Cloud customers want a QoS that enhances compliance with regulations that govern data protection.

Cloud customers face also new challenges to integrate a variety of different cloud services into existing IT infrastructures (Ragowsky et al. 2014). Cloud services as a special form of IT outsourcing can become obsolete overnight due to changes in business strategy (Rai et al. 2009). To quickly adopt and integrate new services, companies seek for partnerships to digitalize their processes and products (Pagani 2013).

Further, when ranking QoS attributes, cloud customers must consider the advantages and disadvantages of possible related technical and managerial QoS attributes on several dimensions. For example, a more detailed contract may have a negative influence flexibility regarding the possibility to carry out speedy changes (Gopal/Koka 2012). Saripalli/Pingali (2011) and Repschlaeger et al. (2013) used point-wise approaches (simple additive weighting and analytical hierarchy process, respectively), which do not consider dependencies between QoS attributes (Kritikos/Plexousakis 2009).

To overcome these limitations, this study investigates how cloud customers respond to environmental changes in 2015 and considers independencies between and within technical and managerial QoS attributes.

6.3 Research Approach

To address our research aim, we needed input from professionals with extensive experience in the cloud computing field and chose the Delphi approach as our research method as it allows aggregation of responses through an iterative process of controlled feedback (Dalkey/Helmer 1963; Okoli/Pawlowski 2004). The Delphi method is recommended when “the problem does not lend itself to precise analytical techniques but can benefit from subjective judgments on a collective basis” (Linstone/Turoff 1975). The Delphi method allowed us to gain insights into the most important QoS attributes and their relative importance as identified by the collective experience of our professional panel (Schmidt 1997) and to consider possible dependencies between QoS attributes (Kritikos/Plexousakis 2009; Saripalli/Pingali 2011; Pare et al. 2013). The Delphi process stops when a reasonable level of consensus or another predefined stop criterion is achieved (Schmidt 1997).

6.3.1 Panel Selection

We recruited professionals with significant work experience in the field of cloud computing to obtain valid and robust results (Okoli/Pawlowski 2004). We located our panel of professionals, responsible for decision-making on CSP selection at their place of employment, at cloud computing workshops and through a special interest group for cloud computing on a social network website. Professionals practicing in this field and known to the researchers were also included. All potential professionals were asked predefined questions regarding their cloud experience and use of cloud deployment and cloud delivery models. To ensure a reliable panel, we excluded novice persons (those with less than one year of cloud experience), private and hybrid cloud users, and cloud service users who use cloud services less frequently than once a day. We screened our professionals to make sure that as many types of industries as possible were included in the study resulting in representation of organizations of different sizes using various types of cloud service models in the sample. An overview of the panel selection criteria is presented in Table 20.

#	Selection criteria	Description
1	Cloud service decision maker	Professionals who are cloud service decision makers.
2	Non-novice person	Professionals with more than one year of cloud experience.
3	Public cloud user	The employing organization uses public cloud services.
4	Frequent cloud service user	Only professionals who use cloud service at least once a day will be considered.
5	Diversity of used cloud service models	At least three types of cloud service models (IaaS, PaaS, and SaaS) should be represented in the sample.
6	Diversity of organizational sizes	Organizations of all sizes (large-, medium-, and small-size organizations) should be represented.
7	Diversity of industries	Panelists should be employed by diverse industries.
8	Diversity of organizations	Panelists should be employed by diverse organizations.

Table 20. Professional panel selection criteria

We invited 32 professionals fitting our selection criteria, of whom 19 participated in the first round of the study resulting in an effective response rate of 59%; no obvious response bias regarding our selection criteria was observed. Our panel had experience with three cloud service models (Infrastructure-, Platform-, and Software-as-a-Service), represented as small-, medium-, and large-sized organizations, and which came from different industries (financial services, manufacturing, software development, railway, media, energy, data analytics, public administration, and wholesale). While some of the panelists were responsible for CSP selection within their company, others served as consultants and were frequently challenged with CSP selection for their customers. Each panelist worked for a different company. The profile of the panel indicates considerable CSP selection experience for diverse service models, industries, and company sizes, thus establishing the credibility of the panel (Table 21).

#	Position	Company category	Geography of operation	Cloud service model	Industry
1	IT-Manager	LO (>250)	Worldwide	SaaS	Energy
2	Business Intelligence	LO (>250)	Germany	IaaS	Media
3	CEO	MO (50-249)	Germany	SaaS	Manufacturing
4	CEO	SO (10-49)	UK	IaaS and PaaS	Financial services
5*	COO	SO (10-49)	Germany, Switzerland, and Austria	SaaS	Communication
6	Consultant (Manager)	LO (>250)	Worldwide	SaaS, PaaS, and IaaS	IT-Consultant
7	Consultant (Partner)	LO (>250)	Worldwide	SaaS, PaaS, and IaaS	IT-Consultant
8	Consultant (Senior)	LO (>250)	Worldwide	SaaS, PaaS, and IaaS	IT-Consultant
9	Consultant (Partner)	LO (>250)	Worldwide	SaaS, PaaS, and IaaS	IT-Consultant
10*	IT-Manager	LO (>250)	Worldwide	SaaS	Software development
11	Project Manager	LO (>250)	Germany	IaaS	Public administration
12	IT-Manager	LO (>250)	Germany	IaaS	Data analytics
13	IT-Manager	MO (50-249)	Germany	SaaS	Financial services
14	IT-Manager	LO (>250)	Worldwide	PaaS and IaaS	IT service
15	Project Manager	LO (>250)	Germany	IaaS and SaaS	Railway
16	IT-Manager	LO (>250)	Worldwide	IaaS and PaaS	Manufacturing
17	COO	SO (10-49)	Germany and Asia	IaaS and PaaS	Software development
18	CEO	SO (10-49)	Germany	SaaS	Wholesale
19*	CEO	SO (10-49)	Germany	SaaS	Software development

* left study after iteration 1 of round 3.

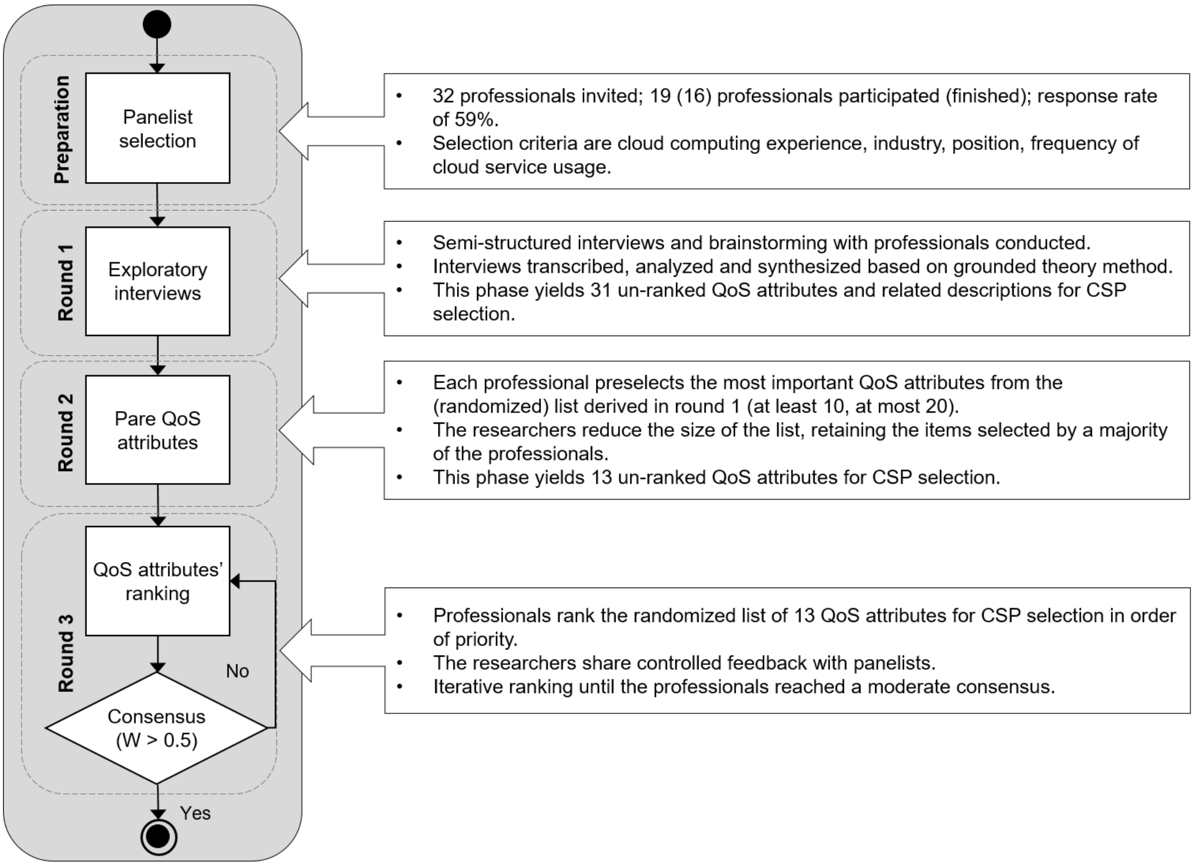
LO = Large-sized organization; MO = Medium-sized organization; SO = Small-sized organization

Table 21. Overview of characteristics of panel professionals

6.3.2 Data Collection and Analysis Method

We followed a modified version of the Delphi method, as proposed by Schmidt (1997), to investigate the relative importance of QoS attributes. Data were collected through brainstorming and semi-structured interviews allowing us to develop a deep understanding of the identified QoS attributes and reasoning behind the participants' individual rankings. Similar to Schmidt et al. (2001), our study design had four stages: the preparation stage and the three subsequent Delphi rounds (Figure 7). We started our first Delphi round in May 2015 and completed the study in October 2015. Activities during the preparation stage included planning of the study and establishment of the professional panel using our selection criteria as described above.

An overview of our research process is shown in Figure 7.



- 32 professionals invited; 19 (16) professionals participated (finished); response rate of 59%.
- Selection criteria are cloud computing experience, industry, position, frequency of cloud service usage.

- Semi-structured interviews and brainstorming with professionals conducted.
- Interviews transcribed, analyzed and synthesized based on grounded theory method.
- This phase yields 31 un-ranked QoS attributes and related descriptions for CSP selection.

- Each professional preselects the most important QoS attributes from the (randomized) list derived in round 1 (at least 10, at most 20).
- The researchers reduce the size of the list, retaining the items selected by a majority of the professionals.
- This phase yields 13 un-ranked QoS attributes for CSP selection.

- Professionals rank the randomized list of 13 QoS attributes for CSP selection in order of priority.
- The researchers share controlled feedback with panelists.
- Iterative ranking until the professionals reached a moderate consensus.

Figure 7. Research process based on Schmidt et al. (2001)

In round 1, brainstorming and semi-structured interviews with each professional were arranged and conducted to identify as many QoS attributes as possible (see Appendix B). While brainstorming enabled us to obtain a large quantity of possible relevant QoS attributes, the semi-structured interviews provided additional information and some QoS attributes not mentioned during brainstorming.

After interviewing the professionals, the gathered information was transcribed, analyzed, and synthesized. To aggregate the findings across all interviews, we adapted the method of Strauss/Corbin (1990) and used open and axial coding to identify all relevant QoS attributes. To ensure consistent coding, two researchers independently read and coded all interview transcripts line-by-line using phrases from the transcripts describing QoS attributes (open coding) and discussed any conflicting results. This open coding process resulted in a list of 69 codes and 360 phrases. The resulting discussions and the rich body of information within the transcripts provided us with necessary background information for the subsequent axial coding (see Appendix C). After completing the axial coding, we reached a final list of 31 unranked QoS attributes.

As members of our panel had different job positions and came from different industries, it was fundamental to assure each professional had the same understanding of each single QoS attribute. To assure common understanding, the panelists were asked to make corrections and validate the attribute descriptions resulting in several changes and clarifications being made to the descriptions. After this clarification process, our panel agreed on the QoS descriptions (see Appendix D).

During round 2, we pared the consolidated list of QoS attributes into a more manageable set for the ranking phase (Okoli/Pawlowski 2004). Following the suggestion by Schmidt (1997), we presented the professionals with a randomized list of the 31 unranked QoS attributes from round 1 and asked each professional to select (not rank) the most important attributes (at least 10 and at most 20 QoS attributes) for CSP selection. We provided a brief definition for each QoS attribute to assure that all professionals had the same understanding of each. All 19 professionals provided responses in round 2. After the responses were consolidated, a cut-off value was defined to yield a list of 12 to 15 items for the subsequent ranking phase (Singh et al. 2009). Using this process, we chose a cut-off value of 60% and identified a pared list that included 13 of the most important QoS attributes.

The pared list was transferred to round 3 of the study for ranking. We sent the manageable list of 13 QoS attributes for CSP selection from the selection round 2 in randomized order to each of our professionals and asked them to rank the QoS attributes in order of priority. We also asked the professionals to explain their reasoning for the chosen ranking. This information was shared with the professionals in subsequent iterations. To measure the degree of consensus among our professionals, we followed the approach of Schmidt (1997) and used Kendall’s coefficient of concordance (W). Kendall’s W is frequently used in Delphi studies and is applied to indicate whether a consensus among the panelists has been reached and the relative strength of the consensus (Schmidt 1997). When Kendall’s W is greater than 0.7, strong consensus has been reached; values between 0.5 and 0.7 indicate moderate consensus, and values less than 0.5 indicate little consensus among panelists (Schmidt 1997). Nineteen professionals participated in the first iteration of ranking in round 3, which yielded a Kendall’s W value of 0.22 indicating relatively weak consensus.

Following Schmidt (1997), we decided to continue the ranking process until the coefficient of concordance indicated a moderate consensus. Therefore, we conducted two further iterations within round 3. This time we provided the following additional information to each professional as controlled feedback: (I) the average rank of each criterion, (II) the ranking given by that professional for each criterion at the prior iteration of ranking, and (III) the percentage of professionals who ranked that criterion within the top 50%. As a fourth controlled feedback (IV), we provided a summary of all comments made by the professionals for each criterion collected within the prior iteration. Similar to Singh et al. (2009), we believed that this additional information would help the professionals to consider their own ranking in light of the group’s ranking, thus providing them the opportunity to adjust their ranking where it made sense to do so. Sixteen professionals participated in the second iteration, yielding a Kendall’s W of 0.32. The Kendall’s W was 0.69 in our third iteration in which 16 professionals participated, suggesting that a moderate level of consensus had been reached. According to the rankings made by the professionals during iteration three of round 3, Kendall’s W almost doubled. However, such improvements in Kendall’s W after round 2 are quite common (Singh et al. 2009; Pare et al. 2013). We believe this result may be because the professionals were able to reflect on their own ranking in light of the panel's ranking by considering the controlled feedback of two iterations. This additional information most likely helped the professionals to reach a group consensus.

6.4 Results and Discussion

In the following, we present results from the first round of our Delphi study and report on the QoS attributes that were derived from the exploratory interviews. We illustrate examples of interview quotes used to produce the list of QoS attributes. We then present the results from the second and third rounds of our Delphi study, where the attributes were pared and ranked. Finally, we provide a CSP selection framework according to a classification of our results.

6.4.1 Identification of Quality-of-Service Attributes

The first round (exploratory interview phase) of our Delphi study included interviews (see Appendix E) and brainstorming. The resulting 31 unranked QoS attributes for CSP selection are listed in Table 22 and briefly described in Appendix F.

No.	QoS attribute	No.	QoS attribute	No.	QoS attribute
1	Assurance statement *	12	Flexibility	22	Ownership *
2	Benchmark *	13	Functionality	23	Personal contact *
3	Business process transparency *	14	Geolocation of servers	24	Process maturity *
4	Certification	15	In-house recommendation *	25	Reputation *
5	Cloud exit strategy *	16	Integration	26	Standard operating environment *
6	Contract	17	Interoperability	27	Support
7	Control	18	Legal compliance	28	Test of solution *
8	Deployment model	19	Market share *	29	Third-party recommendation *
9	External business communication	20	Monitoring	30	Track record
10	Failure preventive measures	21	Open communication	31	Transparency of activities
11	Financial performance *				

* new QoS attributes not represented in earlier lists

Table 22. List of 31 unranked QoS attributes for cloud service provider selection

As our first objective was to develop a list of QoS attributes with a wide coverage of possible QoS attributes, we expected some differences between our list and the combination of previous lists. Given the radical legal, technological developments and changing role of decision makers within the cloud computing market within the past few years, we expected to find that (1) some risk items have remained relatively stable, while (2) others have declined in importance over time. Because previous studies tended to generate QoS attributes according to literature, we expected that (3) the list resulting from our disciplined Delphi approach would contain some unique items not detected in earlier studies.

To address the three points outlined above, we adapted the approach of Schmidt et al. (2001) and compared our list to a merger of other QoS attributes lists from Repschlaeger et al. (2013) and Saripalli/Pingali (2011). A combination of these two lists and our list was therefore used for this comparison. The results of this analysis are presented in Table 22 and illustrated in Figure 8.

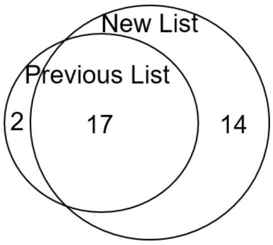


Figure 8. Comparison of QoS attribute lists

The first subset of QoS attributes we consider are those we expected would remain stable over time. Although there were 17 QoS attributes identified by our panel, which could be matched in some way with 31 QoS attributes in the combined list, there is not a strict one-to-one correspondence. As an example, according to our definition (see Appendix F), functionality covers QoS attributes of the combined list, such as security or availability. In that case, functionality serves as a surrogate for some low-level QoS attributes mentioned in the combined list. Nine of these 17 QoS attributes have been identified within each list and could be matched in some way across the lists. Several attributes such as compliance or monitoring possibilities could be directly matched across all lists.

Regarding the second point, our analysis revealed two QoS attributes identified in earlier studies but not represented in our list (and are thus not presented in Table 5). Interestingly, autonomy and graphics agility, not considered QoS attributes in our list, are related to technological issues. It appears that the importance of these attributes has diminished over the past few years, perhaps due to a more mature cloud market.

The third point involves the 14 new QoS attributes identified by the panel but not mentioned in previous studies. Thus, our list of attributes greatly increases the coverage of known QoS factors and suggests that some new elements of QoS attributes have emerged during the past few years, for instance, managerial QoS attributes. Three major groups of QoS factors surface from these 14 new QoS attributes.

Three of the new QoS attributes relate to partnering with cloud customers to co-create value. While cloud resources are exchangeable commodities, cloud customers want a good relationship to co-create value with the CSP. This might have changed in recent years because companies are increasingly challenged to digitalize their processes and products and seek certain platform strategies. Hence, cloud customers need reliable CSP with good financial performance and market share to assure that long-term relationships have a personal contact.

A second major topic deals with lock-in effects. This is an interesting finding as it points out the cloud customers' awareness and proactive behavior to assure flexibility, also in the long-term. To date, cloud services can become obsolete overnight because of changes in business strategy. Therefore, the demand for cloud service exit strategies and standardized operating environment is high.

The third major topic of new QoS addresses how cloud customers bring themselves up to speed on CSPs' data protection capabilities. Laws in place force cloud customers to take responsibility for the cloud services they use and data transferred. To address this issue, cloud customers assure legal compliance by reading assurance statements of the CSP. Further, cloud customers rely on a good reputation of CSP or the recommendation of a third party. Such QoS provides cloud customers indirectly information about the capabilities of a possible CSP to protect data.

6.4.2 Ranking of Quality-of-Service Attributes

In round 2, the professionals pare the list of 31 QoS attributes retaining only, in their opinion, attributes of greatest importance. Table 23 presents the 13 most important QoS attributes as identified by the professionals, their average rank, the Kendall's W value for each ranking iteration in round 3, and the final ranking of the QoS attributes.

QoS attribute	**Iteration 1 average rank**	**Iteration 2 average rank**	**Iteration 3 average rank**	**Final rank**
Functionality	2.95	2.6	1.56	1
Legal compliance	4.79	4.53	2.56	2
Contract	6.42	5.20	3.94	3
Geolocation of servers	5.42	5.27	4.25	4
Flexibility	6.11	6.40	5.75	5
Integration	7.26	7.40	6.88	6
Transparency of activities	7.21	7.07	7.44	7
Certification	8.21	7.20	8.19	8
Monitoring	8.42	8.27	8.75	9
Support	7.89	8.20	9.00	10
Control	8.21	8.67	9.25	11
Deployment model	8.79	9.67	11.56	12
Test of solution	9.32	10.53	11.88	13
Kendall's W*	0.22	0.32	0.69	
* Kendall's W > 0.7 = strong consensus among panelists Kendall's W from 0.5 to 0.7 = moderate consensus among panelists Kendall's W < 0.5 = little consensus among panelists				

Table 23. Ranking from iterations one to three and final ranking of the most important QoS attributes for selecting a cloud service provider

As mentioned, iteration 3 yielded a Kendall's W value of 0.69 indicating that our predefined stop criterion of a moderate consensus was achieved. Because our panel of professionals was highly diverse in regard to the type of cloud service model used, size of company, and type of industry represented, we conclude that a reasonable degree of confidence in the ranking is reached (Schmidt 1997).

To better understand what the most important QoS attributes are, we compared rankings between each iteration. Interestingly, the ranking of the top 5 QoS attributes (functionality, legal compliance, contract, geolocation of servers, and flexibility) remained stable during each iteration. This suggestion of a high and stable consensus regarding these attributes could be interpreted as a universal indicator of the most important QoS attributes during CSP selection decisions.

In contrast, the priority of QoS attributes with a ranking of 6 to 13 slightly changed during each iteration. Hence, our controlled feedback after two iterations might have helped the professional to reflect on their own ranking in light of the overall panel's ranking. Although we reached an overall moderate consensus by the panelists, our results indicate that factors ranked between 6 and 13 might vary individually in terms of their importance during CSP selection decisions.

Finally, the panel considered dependencies between QoS attributes during the controlled feedback. For example, one professional who used domestic cloud solutions mentioned, "[l]egal compliance is connected to geolocation and transparency of activities." Another professional used cloud services located worldwide and remarked regarding the importance of contracts, "[i]n countries where the industry is less regulated, the contracts have to be more detailed." It seems our panel ranked the most important QoS attributes by also considering dependencies between the attributes.

6.4.3 Classification of Quality-of-Service Attributes

To select the right CSP, both technical and managerial QoS attributes must be considered by cloud customers. To provide guidance, we classify our results in the most important technical and managerial QoS attributes according to our interviews and the ontology of Zhou et al. (2007).

Technical Quality-of-Service Attributes	
Attribute	**Classification Motivation**
Functionality	Defines cloud service-related QoS functionalities such as availability or performance attributes.
Flexibility	Defines the latency of the CSP as cloud service-related changes are requested.
Integration	Defines the interfaces, protocols, and characteristics of the cloud service.
Control	Mechanisms comprising tools and approaches enabling individuals to configure and control outcomes of the cloud service.

Managerial Quality-of-Service Attributes	
Attribute	**Classification Motivation**
Legal compliance	Defines the legal environment where data are processed or stored within the cloud service.
Contract	Contracts provide an incentive structure surrounding the cloud relationship including rights and obligations for both parties.
Geolocation of servers	Defines the geolocation where data are processed within the cloud service.
Transparency of activities	Assures that all CSP-related activities will perform as specified by a predetermined set of widely accepted agreements and rules.
Certification	Defines an endorsement from a third party attesting that a (potential) partner adheres to the organization’s policies and standards.
Monitoring	Assures that all cloud service-related transactions will perform as specified by a predetermined set of widely accepted agreements and rules.
Support	The degree to which the vendor provides support to the client while, e.g., evaluating, testing, and selecting services.
Deployment model	Former mechanism to assure data security and privacy.
Test of solution	Provides proof of concept for service quality and interoperability to avoid future service failures and assure interoperability of the cloud service.

Table 24. CSP selection framework based on technical and managerial QoS attributes

The technical QoS consists of attributes (functionality, flexibility, integration, and control) related to operational aspects of the cloud service. The managerial QoS consists of attributes (contract, legal compliance, geolocation of services, transparency of activities, certification, monitoring, test of solution, and support) used for capturing cloud service management information. Overall, both technical and managerial QoS are equally distributed across all QoS attributes priorities (Table 24).

6.5 Contribution to Literature and Practice

The empirical results of this study support cloud customers during CSP selections by identifying the most important technical and managerial QoS attributes for CSP selection as best practices. Usually several CSPs can fulfill cloud customers’ basic requirements (Garg et al. 2013; Schrödl 2012). By considering technical and managerial QoS attributes, cloud customers can determine the “right” CSP to assure future cloud service performance and compliance with laws, policies, and rules (Garrison et al. 2012; Garrison et al. 2015; Weinhardt et al. 2009). Because cloud customers often lack knowledge to determine relevant QoS attributes (Huang/Nicol 2013; Ramacher/Mönch 2014), we provide a list of the most important QoS attributes for CSP selection in 2015. The QoS attributes in the descending order of relevance are functionality, legal compliance, contract, geolocation of services, flexibility, integration, transparency of activities, certification, support, control, deployment model, and test of solution.

6.5.1 Limitations and Future Research Directions

As with any study, the results of the current study must be interpreted in the context of the limitations and constraints regarding generalizability, professional selection, and abstraction level of QoS attributes for CSP selection.

First, the study results are based on the participation of 16 professionals and may not be generalizable to a larger population or prescriptive in nature. However, the rich data resulting from our interviews in combination with the Delphi ranking provide an initial starting point for future research. Being able to analyze results from a larger group of cloud computing decision makers from an extended pool of firms or countries, or for other cloud delivery models (such as private cloud), would be advantageous for future research.

Second, our professionals were not chosen randomly, and we did not attempt to control for the criticality (in terms of data sensibility) of cloud services they used. However, because Delphi studies also require a high effort from participants, using a convenience sample is quite common (Pare et al. 2013). Future studies using a larger, randomized sample controlling for criticality of used cloud services and employing research techniques such as survey designs could enhance generalizability of results.

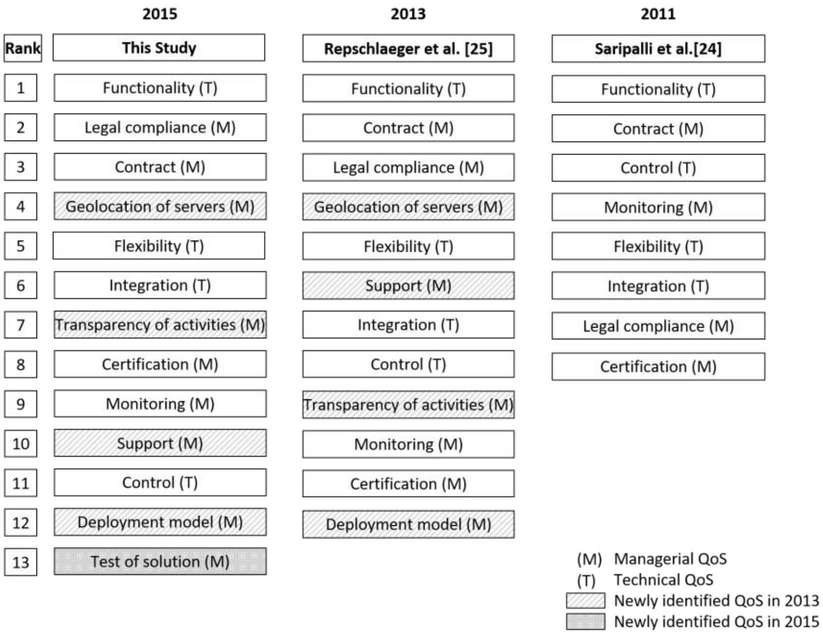
Third, we considered QoS attributes for CSP selection decision on a high abstraction level. To provide further insights, future research might use our results as a research agenda for investigating technical and managerial QoS attributes on a lower abstraction level. Researchers could combine previous results on QoS attributes with our decision framework and focus on the impact of the most important managerial QoS attributes including legal compliance, privacy issues, contract-related aspects, different pay-per-use models, or the impact of geolocation of servers on CSP selection.

Finally, the legal environment is continuously changing. While the Safe Harbor agreement was struck down in 2015, the EU-US Privacy Shield was accepted by the EU in 2016. Our research illustrates a snapshot of 2015 when, for the first time, such a well-known agreement was struck down. Therefore, our study provides important insights about how the relative importance of QoS attributes evolves over time and which cloud market changes take place. Future research might use these insights to further investigate CSP adoption and selection decisions by considering, e.g., cloud security platforms (Schreieck et al. 2016).

6.5.2 Contribution to Literature

On the basis of our identification of the most important QoS attributes (Section 4.2), we identify and compare how the most important QoS attributes differ between 2011 and 2015.

Figure 9 provides an overview of the newly identified QoS and the relative importance of QoS in 2015 (this study), 2013 (Repschlaeger et al. 2013), and 2011 (Saripalli/Pingali 2011).



	2015	2013	2011
Rank	This Study	Repschlaeger et al. [25]	Saripalli et al.[24]
1	Functionality (T)	Functionality (T)	Functionality (T)
2	Legal compliance (M)	Contract (M)	Contract (M)
3	Contract (M)	Legal compliance (M)	Control (T)
4	▨ Geolocation of servers (M)	▨ Geolocation of servers (M)	Monitoring (M)
5	Flexibility (T)	Flexibility (T)	Flexibility (T)
6	Integration (T)	▨ Support (M)	Integration (T)
7	▨ Transparency of activities (M)	Integration (T)	Legal compliance (M)
8	Certification (M)	Control (T)	Certification (M)
9	Monitoring (M)	▨ Transparency of activities (M)	
10	▨ Support (M)	Monitoring (M)	
11	Control (T)	Certification (M)	
12	▨ Deployment model (M)	▨ Deployment model (M)	
13	▩ Test of solution (M)		

(M) Managerial QoS
(T) Technical QoS
▨ Newly identified QoS in 2013
▩ Newly identified QoS in 2015

Figure 9. Relative importance of QoS as identified by this study in comparison to Repschlaeger et al. (2013) and Saripalli/Pingali (2011)[2]

We identify an increasing importance of managerial QoS related to *data protection* aspects. Such QoS attributes are “legal compliance”, “geolocation of servers”, “transparency of activities”, and “deployment model.” According to our professionals, such QoS attributes are important to gain confidence on adequate data protection. While the geolocation of a server affects data protection through local laws in place, the transparency of activities helps cloud customers decide whether data protection mechanisms are compliant with legal and internal requirements. Further, the deployment model helps cloud customers to gain confidence about the separation of companies’ data from third-party data.

During the studies of Saripalli/Pingali (2011) in 2011, of Repschlaeger et al. (2013) in 2013, and our study in 2015, the relative importance of “legal compliance” increased. In comparison to Saripalli/Pingali (2011), Repschlaeger et al. (2013) identified “geolocation of servers”, “transparency of activities”, and “deployment model” as new managerial QoS attributes. Within

[2] To compare how the relative importance of QoS evolved between 2011 and 2015, we used the most important QoS of each attribute, identified the relative importance in comparison to the other attributes within each study, and compared the ranking results with the ranking results of this study.

our study, while the relative importance of "geolocation of servers" and "deployment model" remains important, the relative importance of "transparency of activities" increases.

We assume that the changing legal environment is responsible for the increasing importance of QoS related to data protection issues (Schneider/Sunyaev 2016). Cloud customers have the ability to assure data protection (Goodman 2000). Hence, cloud customers increasingly want QoS to protect their data and be able to maintain compliance with guidelines for data protection.

We identify an increasing importance of QoS related to *value co-creation* between cloud customers and CSP. Such QoS attributes are "flexibility", "integration", and "support." According to our professionals, they look for partnerships to digitalize their processes. Cloud customers value the knowledge of different CSPs regarding the integration of digital products and services. This is particularly important because cloud customers face increasing competition and a need to optimize their value creation.

The relative importance of "flexibility" and "integration" remained stable between 2011 (Saripalli/Pingali 2011), 2013 (Repschlaeger et al. 2013), and 2015 (this study). In comparison to Saripalli/Pingali (2011), Repschlaeger et al. (2013) identified "support" as a new managerial QoS attribute. In our study, the relative importance of the managerial QoS "support" decreased but remained within the top 10 of the most important QoS attributes.

We assume the rising market competition forces cloud customers to establish a partnership with CSP to co-create value (Pagani 2013). Within volatile markets, cloud customer have to quickly adopt their business strategies (Rai et al. 2009). Because of the unforeseen events, existing cloud services can become obsolete overnight (Rai et al. 2009). To compete in such markets, cloud customers need flexible cloud services that are easy to integrate into their IT landscape. To enable a flexible integration of cloud services, cloud customers rely on CSPs' support capabilities and co-create value for their customers (Pagani 2013).

We identified a decreasing importance of technical and managerial QoS attributes related to avoidance of a CSPs' *opportunistic behavior*. These QoS attributes are "contract", "control", and "monitoring". According to our professionals, a huge variety of comparable cloud services are available on-demand. Because of the standardization of cloud services, contracts become standardized and easy to compare. Cloud customers commonly use communities including other cloud customers to gain insights about the accuracy and quality of possible CSPs.

The relative importance of contracts decreased between 2013 (Repschlaeger et al. 2013) and 2015 (this study) but remained within the top 3 of the most important QoS attributes. The relative importance of control decreased between 2011 (Saripalli/Pingali 2011), 2013 (Repschlaeger et al. 2013), and 2015 (this study). The relative importance of "monitoring" also decreased between 2011 (Saripalli/Pingali 2011) and 2013 (Repschlaeger et al. 2013) tremendously but slightly increased in 2015 (this study).

We assume, through the increasing transparency within the cloud market, the possibility of a decrease in CSPs' opportunistic behavior. Companies have access to global and exchangeable cloud resources because of increasing competition in the cloud market (Chen/Wu 2013).

Standardized cloud services and features such as control possibilities enable customers to acquire cloud services from a variety of different CSPs (Truong-Huu/Tham 2014; Lang et al. 2018b). Should a CSP act in a dishonest manner, the cloud customer can quickly change the CSP. Distributed knowledge about the dishonest behavior of the CSP would prevent new cloud customers from acquiring cloud services from them. Cloud customers know that the possibility of CSPs' opportunistic behavior decrease and, therefore, the relative importance of QoS attribute such as standardized contracts or monitoring possibilities decrease.

Finally, we identify the new QoS "test of solution", which is related to *product uncertainty* during CSP selection decisions. According to our professionals, they particularly use a free trial version of cloud services to investigate if the new cloud service fits the existing IT infrastructure and if potential users are able to use such services. This testing procedure helps cloud customers during their CSP selection decision to assess if the cloud service will meet all requirements.

We assume the new identified managerial QoS "test of solution" is required by cloud customers because of the increasing amount of CSP, who offers a variety of unknown cloud services. Cloud customers face product uncertainty during the CSP selection decision due to information asymmetries (Schneider/Sunyaev 2016). Because an increasing amount of CSP enters the cloud market, cloud customers use a test of solution to verify if their requirements are met and the cloud service can be integrated into existing information systems (Yan/Wakefield 2015).

Table 25 summarizes our results about the changes in the cloud environment between 2011 and 2015.

Category	**Changing cloud environment**	**Relevant QoS**	**QoS type**	**Newly identified QoS**
Data protection	Increasing amount of laws, policies, and rules in place increases the importance of data protection	Legal compliance, geolocation of servers, and transparency of activities	Managerial	Yes, partly
Value co-creation	Increasing market competition forces the cloud customer to establish a partnership with CSP	Flexibility, integration, and support	Managerial and technical	Yes, partly
Opportunistic behavior	Increasing transparency within the cloud market decreases the possibility of CSPs' opportunistic behavior	Contract, control, and monitoring	Managerial and technical	No
Product uncertainty	Increasing amount of CSP offers unknown cloud services	Test of solution	Managerial	Yes

Table 25. Changes in the importance of QoS due to changes in the cloud environment

6.5.3 Contribution to Practice

According to our results, the combination of technical and managerial QoS attributes is important during CSP selection to assure future cloud service performance and success. While technical QoS attributes help cloud customers to select the best possible CSP to meet organizational requirements (Wang/Du 2016), managerial QoS attributes verify the capabilities of the CSP, increase predictability in the cloud service exchange relationship, and provide confidence in decision-making (Zhou et al. 2007; Ghosh et al. 2015; Huang/Nicol 2013). As cloud customers need to be confident to conduct optimal CSP selection decisions and not all necessary information for decision-making is available, they use managerial QoS attributes. For example, cloud customers are unable to predict future availability of the cloud service because of a lack of complete information. To assure future availability, cloud customers use contracts including predefined penalties in case the CSP does not offer the services as stipulated in the contract. The combination of technical and managerial QoS attributes is particularly important to assure future performance and conduct optimal CSP selection decisions (Table 24).

As our results stem from consensus among professionals, they provide not only guidance for new and existing cloud customers during CSP selection but also information for CSP to better address cloud customers' needs.

Our results provide a starting point for new cloud customers to identify relevant QoS attributes when making CSP comparisons and during the CSP selection process. Using our results, new cloud customers can compare and select CSP by focusing on the most important technical and managerial QoS attributes. Because our professional panel was not able to reach a strong consensus on the importance of QoS attributes, persons charged with making cloud decisions should adapt this list to better accommodate individual requirements.

Existing cloud customers are informed about CSP selection because the relative importance changed during 2011 and 2015. Therefore, in line with new cloud customers, existing cloud customers get an updated guidance during CSP comparison and selection decisions.

Our results can also assist new and existing cloud customers to select adequate control mechanisms during use of cloud services. While the list of the most important QoS attributes is important when making CSP selection, several managerial QoS attributes can also help cloud customers to control CSP by using contracts, transparency of activities, monitoring, and certificates. While contracts provide a tool to implement predefined penalties in case a CSP not provide the services as stipulated in the contract, transparency of activities, monitoring, and the continuance of certificates may provide cloud customers with some control over the CSP. From a CSP perspective, these results provide a better understanding about cloud customers' needs during CSP selection decisions and required control mechanisms during cloud service usage.

Cooperation with third parties and the cloud customer seems important for CSP. While several attributes are associated with the offered cloud service itself, our results show that CSP should also focus on QoS attributes such as geolocation of services or certification requiring cooperation with third parties. Geolocation of services not only defines QoS attributes such as latency but also influences legal compliance requirements of customers (Ramgovind et al. 2010). IaaS providers should consider data centers in different countries, while PaaS and SaaS providers might use different IaaS service providers in different countries if they themselves do not offer an adequate infrastructure. Certification of cloud services needs an endorsement conducted by a third party (Sunyaev/Schneider 2013). CSPs might use such endorsements not only to address customers' needs but also to identify potential improvements through an independent third party. Furthermore, CSP should establish suitable relationships with cloud customers using features such as support possibilities to co-create value. Overall, to address customers' needs, CSPs might consider third parties to address customer compliance, latency, or support requirements, or to extend transparency within their services.

Our results provide guidance for CSP regarding required control mechanisms. Cloud customers' demand transparency of CSP' activities, monitoring solutions, and up-to-date certificates. Therefore, CSP should implement and communicate these mechanisms to satisfy existing cloud customers and as a means of acquiring new customers. As a communication example, CSP could promote these mechanisms on their webpage to address customers' needs during their CSP selection and control process.

6.6 Conclusion

Using an exploratory Delphi study design, we investigated the most important QoS attributes for the selection of CSP as identified by a panel of professionals. Through consensus, we identified the 13 most important QoS attributes for CSP selection and ranked their importance in 2015. We further showed that our results for QoS attributes comprise technical QoS attributes and managerial QoS attributes, both of which are important during CSP selection.

Our main contribution to what is already known about CSP selection is threefold. First, our results show that cloud customers require an extensive variety of managerial QoS attributes during CSP selection. This finding supports prior research on cloud customer uncertainty in an ever-changing cloud environment. Second, a comparison of the most important QoS attributes in this study with those reported in previous studies identifies the following four key changes that take place within the cloud market: (1) The importance of increasing data protection; (2) The cloud customer's pursuit of value co-creation CSP; (3) The possibility of a decrease in CSPs' opportunistic behavior; and (4) Product uncertainty remains a major problem during CSP selection. Third, we contribute to practice by providing a comprehensive overview of the most important technical and managerial QoS attributes to be considered when making cloud computing investment decisions. On the one hand, (potential) cloud customers get informed during CSP selection decision what the relevant QoS attributes are. On the other hand, our results show CSPs which QoS attributes and related control mechanisms are demanded from a customer perspective.

To conclude, given the ever-changing cloud environment, our results contribute to research and practice by pointing out the most important QoS attributes as identified by cloud customers in 2015. Further, our study provides a comparison of the most important QoS attributes with those as reported in previous studies. We hope that this study provides a starting point for future information systems research to further elaborate cloud decision criteria and dynamics that occur in the cloud market.

7 Perceived Control and Privacy in a Professional Cloud Environment

Title	Perceived Control and Privacy in a Professional Cloud Environment
Authors	Lang, Michael* (michael.lang@in.tum.de) Wiesche, Manuel* (wiesche@in.tum.de) Krcmar, Helmut* (krcmar@in.tum.de) *Technische Universität München, Chair for Information Systems, Boltzmannstraße 3, 85748 Garching, Germany
Publication	Hawaii International Conference on System Sciences (HICSS)
Status	Accepted
Contribution of First Author	Problem Definition, Research Design, Data Analysis, Interpretation, Reporting

Table 26. Fact Sheet Publication P4

Abstract

Cloud customers need to assess whether their cloud service provider offers high-quality services and handles sensitive information confidentially. Privacy protection is therefore a major challenge during cloud sourcing. Although cloud customers want control over their sensitive information, they have limited resources to do so. They therefore consider other control agents, such as certification authorities or collectives, but the effectiveness of these groups to ensure privacy protection is unknown. This study differentiates between three control agents (personal control, proxy control, and collective control) and investigates the influence of these agents on cloud customers' perceived control over sensitive information to protect privacy during cloud sourcing. Results show that proxy and collective control influence cloud customers' perceptions, but personal control does not. Therefore, only external control agents, who can apply sanctions, are perceived as being able to effectively protect privacy.

7.1 Introduction

Cloud computing is commonly used to gain on-demand network access to a shared pool of managed and scalable IT resources (Mell/Grance 2011; Böhm et al. 2010). The volume of sensitive information obtained (such as personal data) within this environment has increased exponentially, as an increasing number of companies considers personal data to be a corporate asset (Schwartz 2004, 2056). However, prior to the transfer of personal data or extending the use of sensitive information, companies need to assure customers that their cloud service provider has adequate security and privacy protections in place (Goodman 2000).

Cloud customers have limited means to assess as to which cloud service provider offers high-quality services and handles sensitive information in a confidential manner, and therefore, security and privacy concerns considerably restrict the adoption and expansion of cloud platforms (Sunyaev/Schneider 2013; Heidkamp/Pols 2017).

Cloud customers are more likely to adopt cloud platforms if they are able to reduce their perceived privacy risks by ensuring that appropriate control exists over the sensitive information they provide (Benlian/Hess 2011). However, they often have limited resources to adequately evaluate the security provided to protect their sensitive information in a cloud environment (Schneider/Sunyaev 2016). Simultaneously, customers desire certain outcomes, such as a positive relationship and privacy protection (Schneider/Sunyaev 2016; Henderson/Lee 1992). In addition to personal control, proxy control (such as the certification of authorities) or collective control (as a member of a group to protect privacy) are often considered when selecting a cloud (Gregory/Keil 2014; Johnson 1974). These control agents can be differentiated with respect to their effectiveness in achieving the required amount of privacy protection (Henderson/Lee 1992), but such considerations are extremely challenging for cloud customers when selecting appropriate and effective control agents (Wiener et al. 2016; Gregory/Keil 2014).

In this study, we adopt a psychological control perspective to investigate the types of control agents that customers consider to be effective in protecting privacy in a cloud environment. More specifically, we adopt a psychological control theory that includes three control agents (personal control, proxy control, and collective control) and investigate the effect that these agents have on cloud customers’ perceptions of privacy in a cloud environment. Using a survey study approach, we seek to answer the following research question: *What kind of control agents do cloud customers consider capable of protecting the privacy of their sensitive information?* Our findings highlight the importance of external control agents in influencing perceived privacy protection, and the intention that such agents have in expanding cloud services by the mediating effect of perceived control over sensitive information.

This paper describes the theoretical background relating to privacy as an inhibiting factor in adopting cloud services and discusses privacy control agents. On the basis of this theoretical background, we develop our hypotheses on the relationship between the differing control agents used to perceive control and to protect privacy that customers have of such agents. Furthermore, we describe our research methodology and choice of operational construct, present intended theoretical and practical implications of our findings, and finally conclude the results of research.

7.2 Theoretical background and hypotheses

7.2.1 Privacy as a major inhibitor for cloud adoption and extension

Cloud computing is “a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources” (Mell/Grance 2011). In this respect, computer resources refer to hardware, development platforms, and applications (Böhm et al. 2009) that “can be rapidly provisioned and released with minimal management effort or service provider interaction” (Mell/Grance 2011). Cloud customers use these resources to process, transfer, and store sensitive information, such as personal data from customers, and to gain advantages with respect to costs and flexibility (Mell/Grance 2011). The receiving party (the cloud service provider) thus needs to have adequate privacy protection in place before cloud customers can feel safe about transferring sensitive information (Goodman 2000).

Security and privacy concerns serve as major inhibitors in adopting cloud and its subsequent expansion. Cloud customers have limited means to assess as to which cloud service provider offers high-quality services and can handle sensitive information in a confidential manner (Sunyaev/Schneider 2013; Benlian/Hess 2011; Lang et al. 2016). After selecting a cloud service provider, the customer transfers direct control of their sensitive information with no accurate knowledge of how exactly this provider will secure data and maintain associated confidentiality (Benlian/Hess 2011). As a result, cloud customers perceive that they have a loss of control over their data, and they regard cloud computing as an uncertain environment (Schneider/Sunyaev 2016). To overcome these uncertainties, cloud customers seek mechanisms to assure and maintain control, such as certification of cloud services, privacy policies, or legal regulations (Sunyaev/Schneider 2013; Yang/Tate 2012).

Cloud sourcing practices involve major management decisions, and it is important to understand the associated (cognitive) processes influencing the behavior of cloud customers (Benlian/Hess 2011). In this respect, Benlian/Hess (2011) investigated the sourcing opportunities of cloud sourcing and the risks facing decision makers. They concluded that cloud customers are more likely to increase cloud adoption, if they can reduce any perceived privacy risks through appropriate control over sensitive information.

In this study, we adopt a control perspective to clarify how cloud customers evaluate controls in place to ensure that their sensitive information and privacy are protected during cloud sourcing.

7.2.2 Privacy control in a cloud environment

Several behavioral scientists have emphasized the importance of control in relation to investigating privacy, where privacy is defined as an individual’s ability to control the terms by which their sensitive information is acquired and used (Westin 1968; Warren/Brandeis 1890; Pavlou 2011). Therefore, privacy is viewed as “control over or regulation of, or more narrowly, limitations on or exemption from scrutiny, surveillance or unwanted access” (Margulis 2003).

According to Johnson (1974), individuals use control to directly or indirectly attain privacy-related outcomes. In addition, individuals strive for control to motivate others to act in a way that is consistent with their privacy goals.

There are two research dimensions in control literature, which respectively focus on “what” control activities are used and “how” controls are enacted (Wiener et al. 2016). Prior studies have mainly focused on which control dimensions are used, and have shown that control activities are moderated by context factors, such as controller knowledge or boundary-spanning activities (Tiwana/Keil 2009; Kirsch 1997). The question as to how controls are enacted determines the effectiveness of control activities, and researchers have investigated the ability of the controller to align control activities with a current situation or in relation to past experiences (Heumann et al. 2015; Remus et al. 2016; Wiesche et al. 2015). This control dimension considers contrasting control styles (collaborative versus authoritative), both of which compete in complex situations (Heumann et al. 2015), such as protecting privacy during cloud sourcing.

Individuals use direct or indirect controls to protect privacy in a cloud environment. The power and ability to influence others (controller) influences the use of a particular control style (Wiener et al. 2016). The cognitive and behavioral limitations of individuals often lead one to limiting oneself to a single style that fits best with the beliefs and skills of others (Gregory/Keil 2014). To compete with a complex situation and benefit from different control styles, individuals conduct controls through not only themselves acting as a control agent (direct control) but also other control agents (indirect control) in order to control a desired outcome such as privacy protection (Gregory/Keil 2014; Johnson 1974). Both direct and indirect controls influence an individual’s perceived control over a certain situation (Du et al. 2007).

7.2.3 Types of control agents in cloud computing

Depending on the set priorities, a cloud customer chooses control agents that deliver a desired outcome (Wiener et al. 2016). However, control agents differ in their effectiveness with respect to reaching a desired outcome, such as enabling a positive relationship and protecting privacy (Henderson/Lee 1992). While an individual cloud customer who acts as a control agent may prefer using collaborative control styles to protect his or her privacy and maintain a positive relationship with the cloud service provider, other control agents (such as certification authorities) instead rely on authoritative control styles that focus on privacy protection. This situation can be challenging for a cloud customer when searching for an effective control agent (Wiener et al. 2016; Gregory/Keil 2014).

In psychology, the construct of control has been treated as a perceptual construct because it is of greater interest than actual control when predicting behavior (Skinner 1996). For example, perceived control has been identified as a powerful factor that influences an individual’s risk perception and IT decision-making during IT projects (Du et al. 2007). The conceptualization of perceived control is therefore a cognitive construct, and as such it may be subjective (Langer 1975). Perceived control refers to an individual’s beliefs regarding his or her ability to affect changes in the environment in a desired direction (De Charms 2013). This study investigates the effectiveness of control agents based on cloud customers' perceived control over sensitive information.

On the basis of Yamaguchi (2001) work on the differentiation of control agents, we hypothesize that cloud customers are able to exercise personal control, proxy control, or collective control over their sensitive information to protect privacy (Table 27).

Control agent	Controller	Privacy protection mechanism example
Personal control	Individuals	Monitoring, privacy policy
Proxy control	Powerful authorities	Certification, legislation
Collective control	Collective	Reputation

Table 27. Control agents based on Yamaguchi (2001)

7.2.3.1 Personal control

Individuals strive for primary control over their environment when they exercise personal control through individual self-protective actions (Weisz et al. 1984). Such a mechanism empowers cloud customers with direct control over the way in which sensitive information may be gathered by cloud service providers. Literature on privacy describes two major types of individual self-protection approaches (Culnan/Bies 2003; Milne/Culnan 2004; Son/Kim 2008; Lang et al. 2017) - technological and non-technological control enactments.

Within an online environment (for example, in the context of cloud computing), users have the possibility of using privacy-enhancing technologies, such as user identification, authentication systems, or security features (for example, SSL connections or access management). As a result, cloud customers are able to configure an individual level of security to protect sensitive information (Xu et al. 2012b).

Non-technological control enactments include mechanisms such as privacy policies provided by the cloud service provider (Xu et al. 2011). In this regard, cloud customers can be informed about the choices available for the way cloud service providers use the information collected. However, technological control enactments are identified as being more powerful than non-technological control enactments (Son/Kim 2008), whereas non-technological control enactments have been identified as being capable of influencing the control perception of controllers within information systems (Xu et al. 2011; Xu et al. 2012b). We therefore predict that personal control via privacy-enhancing technologies and privacy policies will enhance cloud customers' perceptions with respect to control over their information. Our hypothesis in this respect is as follows:

> *Hypothesis 1 (H1): Personal control mechanisms are a secondary outcome of privacy-enhancing technologies and privacy policies enhance cloud customers' perception of information control.*

7.2.3.2 Proxy control

Proxy control is an institution-based control mode wherein powerful authorities act as control agents (Bandura 2001). With proxy control, individuals attempt to align themselves in order to be able to gain control through powerful others (Xu et al. 2012b). Normative rules about organizational behavior are defined and promulgated through active participation in a wide array of events, such as audits or legal investigations organized by certification authorities or government legislators (Son/Benbasat 2007; Lang et al. 2016, 2017). Individuals believe that organizations subscribing to the professional publications of these associations learn acceptable norms of practices and affect the behavior of their organization accordingly (Son/Benbasat 2007). In addition, it is believed that if organizations misbehave in terms of these norms, they will be punished by the powerful authorities (Bandura 2001). Within a cloud context, cloud customers rely on certification authorities and governmental regulations to exercise proxy control over their sensitive information (Schneider/Sunyaev 2016).

Third-party certification is defined as a "process in which a third-party formally confirms that a product, process or service conforms to a set of predefined criteria" (e.g., a certification scheme) (Schneider/Sunyaev 2016). These certifications provide independent verification of a provider's trustworthiness and its ability to protect information. This independent verification is usually provided by knowledgeable and powerful authorities capable of enforcing external sanctions (for example, certificate termination) when cloud service providers are in breach of compliance with a certification scheme (Oezpolat et al. 2013).

Some countries have established legislative efforts to protect sensitive information from unintended access and usage. The legal system, therefore, is a powerful control mechanism for the exercise of social control as it ensures that offenders are punished (Tittle 1980; Lang et al. 2017) and thus deters potential offenders in the case of illegal behavior.

With respect to the deterrent effectiveness of certification authorities and legal systems, information systems studies have identified the positive effects of certificates and laws in the protection of sensitive information within an online environment (Xu et al. 2011; Lowry et al. 2012; Lang et al. 2017). Therefore, in this study, we predict that proxy control via third-party certification and an appropriate legal environment increases cloud customers' perception of information control. We therefore construct our second hypothesis as follows:

> *Hypothesis 2 (H2): Proxy control mechanisms, as a secondary outcome of third-party certification and legislation, enhance cloud customers' perception regarding information control.*

7.2.3.3 Collective control

In collective control, an individual attempts to control the environment as a member of a group or collective, in which the group or the collective serve as an agent of control (Bandura 2001). Collective control is implemented by promulgating common values, beliefs, and philosophies within the collective (Kirsch 1997). The collective propagates norms and values resulting in a group of individuals who share a common ideology, who have internalized a set of values, and who are committed to the collective (Kirsch 1997). If outsiders do not adhere to those norms, the collective control agent can sanction outsiders through informal mechanisms. In collective control, responsibility (as well as agency) is diffused among actors (Latané/Darley 1970).

Collective controls have been identified as important collaborative control styles in situations when the individual is unable to observe the outsider's behavior (Kirsch 1997; Wiener et al. 2016). Within a cloud environment, cloud computing may be considered an uncertain environment in which transparency is limited (Weinhardt et al. 2009). In this respect, collective control styles are also important in an inter-organizational context.

Reputation is considered to play an important role in uncertain environments, where the information conveyed by reputation helps reduce social uncertainty among individuals (Schwarz et al. 2009). Reputation, however, plays another role in reducing social uncertainty, where it often works as a sanction mechanism against dishonest deeds (e.g., reputation as hostage) (Shapiro et al. 1992). Organizations may refrain from misconduct because they fear possible negative consequences with respect to their reputation (Shapiro et al. 1992; Yamagishi/Yamagishi 1994). This sanctioning role of reputation is part of the mechanisms used to protect privacy; it directly reduces the incentive of the owner of the reputation to act dishonestly (Yamagishi/Yamagishi 1994; Lang et al. 2017).

In summary, the information aspect of reputation makes the recipient confident in adapting cloud services and revealing sensitive information. This leads to an enhancement of the consumer's perceived control over sensitive information. In this study, we therefore predict that collective control based on the reputation of the cloud service provider increases the cloud customers' perceived information control. Our hypothesis in this respect is as follows:

> *Hypothesis 3 (H3): Collective control via reputation leads to increased cloud customers' perceived control over sensitive information.*

7.2.4 Information control and privacy

In accordance with previous research, we conceptualize information control as a perception and define it as being an individual's belief in the ability to determine the extent to which sensitive company information, such as personal data from customers, or private information will be released within a cloud environment in an unintended way (Dinev et al. 2013). Prior literature differentiates between two types of control important in a privacy context: control over information disclosure and control over information use once the information has been obtained (Culnan/Armstrong 1999; Spiekermann 2005). Most commonly, providers within the internet address the first dimension by offering granular privacy settings (Hoadley et al. 2010), which limit the accessibility of sensitive information to other members and third parties. However, it has been suggested that individuals feel they have a higher level of privacy when they have a sense of information control (Culnan/Bies 2003). Recent studies on privacy suggest that a loss of information control is central to the perception toward privacy invasion (Dinev et al. 2013).

Accordingly, in this study, we hypothesize that perceived information control is positively related to privacy, as follows:

> *Hypothesis 4 (H4): Cloud customers' perceived information control positively affects privacy.*

7.2.5 Privacy and cloud customers' intention to expand cloud service

The theory of reasoned action asserts that attitudes toward behavior are generally accurate predictors of an individual's behavioral intention in an information system environment (Pavlou/Fygenson 2006). Applying the theory of reasoned action to the cloud expansion context, we hypothesize that cloud service expansion intention is determined by a cloud customer's privacy. Privacy has an influential role in IT expansion and information disclosure behavior and is supported at the individual and organizational level in different application contexts. For example, e-businesses will be used if customer privacy is protected (Xu et al. 2012a). At the organizational level, privacy has been found to be an important construct that enables online transactions and the transference of data to an external partner (Goodman 2000).

Therefore, in this study, we hypothesize that cloud customers' privacy is positively related to the expansion of the usage of cloud services, as follows:

> *Hypothesis 5 (H5): Cloud customers' privacy positively affects their intention to expand their use of cloud services.*

Figure 10 provides an overview of the hypotheses defined in our study.

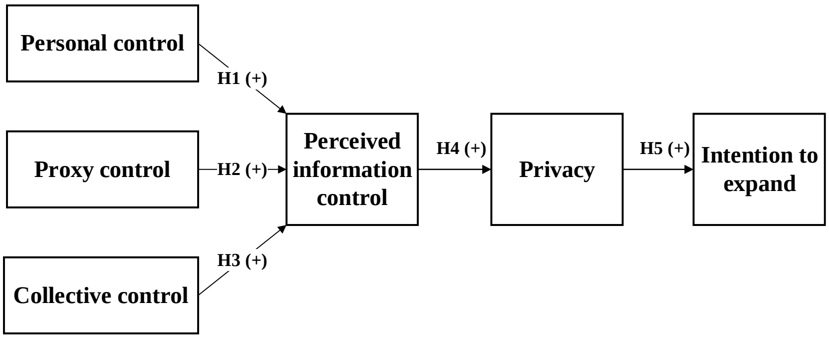


Figure 10. Cloud privacy research model

7.3 Methodology

7.3.1 Sample

To enable ease of design without sacrificing rigor, we implemented our research design within a professional cloud environment to match our target population (Siponen/Vance 2014). We empirically tested our research hypotheses using the data collected through a survey that included items for the constructs specified in the model. The sample of our survey was drawn from a market research company, Digital Intelligence Institute (dii) between September and November 2016; dii is a leading research company studying digital developments within Germany.

To increase the external validity of our study, dii did not constrain the sample to specific industries or to firms of a specific size, and instead drew a random sample from the entire population of cloud decision makers within their database. The survey questionnaire was mailed to the most senior IT executive of each firm (e.g., to the chief information officer, the vice president in charge of IT, or the vice president in charge of business), along with a letter outlining the purpose of the research and soliciting participation.

7.3.2 Scale development

Scale development for the constructs (Table 28) was based on an extensive survey of literature on privacy and psychological control. We adapted validated standard scales and constructs for our use as far as possible. Table 2 provides the constructs used and a summary of the sources used to draw items for scales. All questions (except those regarding legislation) were answered using a Likert scale ranging from 1 to 5, with 1 representing the lowest score as “completely disagree” and 5 representing the highest score as “completely agree”; legislation questions were answered using a Likert scale ranging from 1 to 5 as well but with 1 representing the lowest score as “very low” and 5 representing the highest score as “very high” on the item scale.

Several control variables were added to control for the results affected by extraneous factors. These included participants’ experience of cloud, the deployment model used by a specific cloud service, and whether personal data are processed within this specific cloud service.

To avoid potential language-barrier problems, the survey was provided in German. However, to check for translation bias within measurement items, a back-translation technique was employed wherein two different translators translated the German questionnaire back into English (Bhattacherjee/Park 2014). The back-translated items had a high degree of correspondence with the original English items, thereby assuring a relative lack of translation bias.

Construct		**Source**
Intention to expand cloud services		Benlian/Hess (2011)
Privacy		Dinev et al. (2013)
Perceived information control		Xu et al. (2011)
Personal control	Privacy policy	Xu et al. (2011)
	Privacy-enhancing technology	Hossain/Prybutok (2008)
Proxy control	Legislation *	Koh et al. (2012)
	Third-party certification	Kim et al. (2015)
Collective control	Reputation	Doney/Cannon (1997)

* Two additional self-developed constructs are considered to determine the influence of legislation.
In your opinion, how effective are the laws and regulations in the supplier’s country concerning the following activities?

- Ensuring data privacy in the cloud.
- Ensuring data security in the cloud.

Table 28. Construct operationalization

7.3.3 Survey administration

The current study utilized a "key informants" methodology for data collection, which is a popular approach in empirical information systems studies (Pinsonneault/Kraemer 1993). In organizational survey research, targeted respondents assume the role of key informants and provide information on a particular unit of analysis by reporting on group or organizational properties. However, if a respondent lacks appropriate knowledge, the results can be confusing and may lead to erroneous conclusions. Therefore, it was important within the context of this study to identify respondents who were involved with and were most knowledgeable about cloud services. Consequently, we used a clear definition of cloud computing in the introduction to our survey.

We also indicated that the survey should be completed by the most senior executive available with a good overview of the organization's stance on cloud services. In addition, to increase the content validity of the responses and avoid social desirability bias, we asked respondents to complete the questionnaire with reference to one specific cloud service (e.g., CRM or storage) that they used or were familiar with.

To foster participation and reduce self-reporting bias, all participants were offered a report on their company's position compared with that of others of a similar size and industry. Finally, a pre-test assisted us in the development of both the content and the format of specific questions presented in the survey. Twenty practitioners from various industries known by dii evaluated the results, and we also employed two academics who are experts in cloud computing research.

In total, 109 usable responses (25% of the total customers with a cloud experience of more than three years, 38% with an experience of 1–3 years, and 37% with an experience of less than one year) were available for data analysis. The total sample included companies using cloud deployment models that were 55% public, 25% hybrid, and 20% private. In addition, 76% of the companies processed personal data within the cloud service, whereas 24% did not.

7.4 Data analysis and results

7.4.1 Measurement model

To assure validity of the constructs used, we adopted constructs used in previous studies. Our measurement model was validated using the standard procedure of Straub (1989), and to assess the convergent and discriminant validity of items, the items of the scale were pooled into a related domain. While convergent validity was determined both at the individual indicator level and at the specified construct level, discriminant validity was assessed by analyzing the average variance extracted and inter-construct correlations.

Results showed that all the factor loadings were significant, suggesting convergent validity. All constructs met the threshold value for the average variance extracted (AVE > 0.50) and Cronbach's alpha (alpha > 0.70), as suggested by Straub (1989). For the discriminant validity of latent variables, the square roots of AVEs exceeded inter-construct correlations that were negligibly low between independent constructs. In addition, composite reliability (CR) was calculated and evaluated for each construct; all constructs were found to have a CR that was significantly above the cut-off value of 0.70. In summary, the quality of the measurement model was proven to be satisfactory.

Following the proscribed procedures of MacKenzie et al. (2011), we also calculated the AVE for each second-order construct (personal control and proxy control) by averaging the square of each first-order sub-dimension's standardized loading on the second-order construct. All AVE values were found to exceed the threshold of 0.50, indicating that (on an average) the majority of the variance in first-order dimensions was shared with second-order constructs.

7.4.2 Structural model

We used SmartPLS 3.0 to validate the structural model and to test the hypotheses using the bootstrapping (1000 resamples) method. The second-order personal control and proxy control constructs were estimated using the factor scores of their first-order dimensions as reflective indicators (see Wright et al. (2012)).

Our findings support most of the primary hypotheses of the study (H2, H3, H4, and H5). Proxy control (β = 0.54, t = 6.34) and collective control (β = 0.27, t = 2.93) are positively related to perceived information control and explain 47% of its variance. In turn, perceived control (β = 0.66, t = 12.98) is positively related to privacy and explains 44% of its variance. Finally, privacy (β = 0.48, t = 5.40) is positively related to the intention to expand cloud service with an explanation power of 23%. In contrast, the relationship between personal control (t = 0.20) and perceived information control is not significant at a 5% level, and therefore, H1 is not supported. However, none of the control variables significantly affect perceived control or privacy. Figure 11 illustrates the final results obtained from the research model.

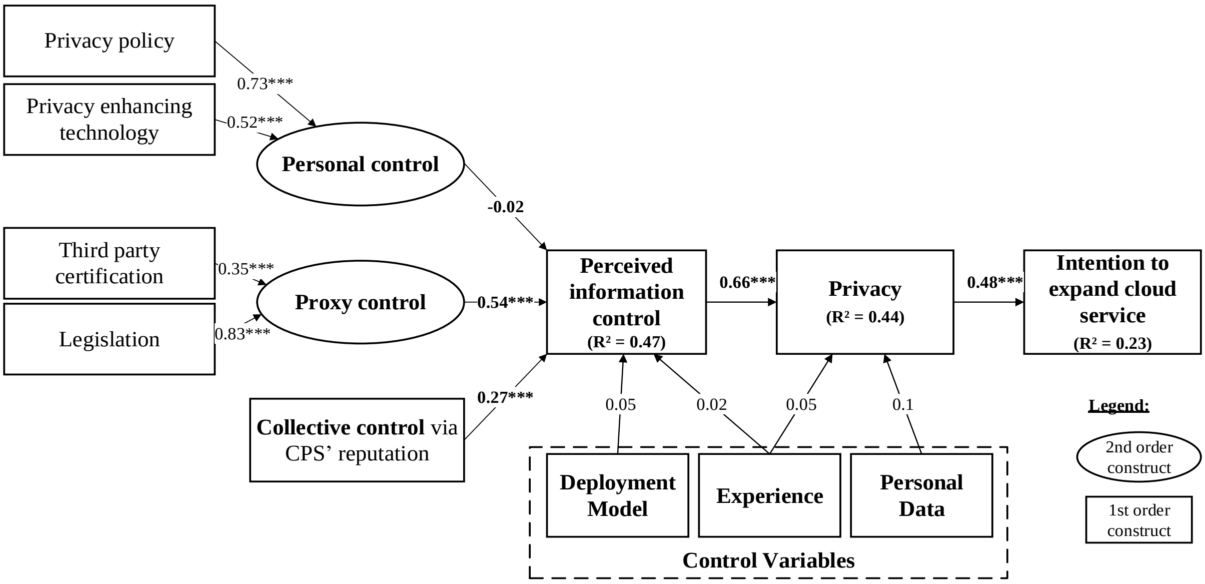


Figure 11. Cloud privacy research model results

7.4.3 Mediation test

In our theoretical model, we posited that perceived information control would mediate the relationship between control agents and privacy. To test this mediation, we conducted a Sobel test, which is a method for assessing indirect affects, and is considered superior (e.g., it provides a better balance between Type I and Type II errors) to the traditional Baron-Kenny mediation test (Detert et al. 2008). We then conducted the Sobel test for the indirect effects of proxy control and collective control on privacy through perceived information control using Preacher's online Sobel test calculator (http://quantpsy.org/sobel/sobel.htm). The Sobel test statistics were significant for (i) the relationship between proxy control and privacy ($z = 5.54$; $p < 0.001$) and (ii) the relationship between collective control and privacy ($z = 4.78$; $p < 0.001$), thereby suggesting that perceived information control plays a mediating role between control agents and privacy.

7.5 Discussion, implications, and limitations

7.5.1 Discussion

Results of this study provide insights into effective control agents operating within a cloud environment. This study differentiates between three control agents (personal control, proxy control, and collective control), and investigates their influences on cloud customers' perceived control over sensitive information and privacy during cloud sourcing.

Although proxy and collective control influence cloud customers, we identified no support from the customers used in our sample for personal control. Hence, only external control agents, which are known to be able to apply sanctions, are perceived to be effective. Furthermore, this study identified the mediation effects of perceived information control between control agents and privacy.

7.5.2 Implications

Our findings have important implications for theory and practice. First, we have extended available literature on privacy by identifying perceived information control as a mediator between control agents and privacy within a professional cloud environment. Research on privacy has previously been conducted mainly within a consumer context (Dinev et al. 2013), although professionals also struggle with privacy issues (Goodman 2000). Our findings provide evidence of the importance of privacy within a professional context and demonstrate the importance of considering the mediating effects of control perception when investigating privacy protection through different control agents and the privacy protection mechanisms used.

Second, we analyze cloud sourcing decision-making by investigating how individuals' perception of control and privacy influences their purchasing decisions (Lang et al. 2017). We demonstrate how cloud customers control sensitive information and ensure privacy within a cloud environment. Such findings are vital for cloud research because they show how different actors influence the cloud sourcing decisions made by cloud customers.

Third, our results extend literature on control by considering different control agents. In line with Gregory/Keil (2014), we argue that although different control agents are important, the differences between their effectiveness should be considered. Furthermore, many studies focus on the perspective of the controlee and investigate if the controlee perceives that the enacted controls are appropriate (Heumann et al. 2015; Remus et al. 2016; Tiwana/Keil 2009). We extend this view by investigating the control perception of a controller with respect to the effectiveness of the controls enacted through control agents. According to our findings, even if controllers have limited resources to control others, additional means of control are available by considering external control agents. Hence, we extend the known literature on control by providing a third dimension “who controls?” which should be considered when investigating enacted controls.

This research also has managerial implications. Our findings contribute to the knowledge used by cloud customers, cloud service providers, legislative and certification authorities, and the society as a whole, by determining effective control agents that influence decision-making in a cloud environment.

Our results assist cloud customers in identifying appropriate controls to assure that a cloud service provider has adequate security and privacy protection in place. For cloud service providers, our results indicate as to which mechanisms are appropriate for use in protecting privacy from a customers’ perspective. Our findings also provide governments, certification authorities, and the society with feedback on the effectiveness of their endorsements. It is considered that these groups might use our results to improve their services and employ reliable and reputable certification authorities, or to consider further channels to share opinions and information on the reputation of cloud service providers.

7.5.3 Limitations

This study was conducted in Germany. Therefore, researchers have to be careful when attempting to generalize the results to other social, economic, legal and cultural environments. Privacy is a relative concept and may be related to cultural values (Kim et al. 2015); what is considered private in one culture or legal region may not be considered private in another. For example, people in the U.S. tend to take a “privacy pragmatist” perspective, whereas Europeans (including Germans) are concerned about their privacy and are more likely to take the perspective of “privacy fundamentalists” (Galanxhi/Nah 2006).

Furthermore, we acknowledge that other critical factors are relevant, such as the strategic importance of cloud services, the home country of a cloud customer, or how trust affects cloud customers privacy perception and expansion decisions. However, our results show that privacy influences the decisions made by cloud customers when extending cloud services, and therefore demonstrates important insights into how cloud expansion decisions are made.

7.6 Conclusion

Results of this study provide insights on effective control agents within a cloud environment. We found that cloud customers seek control over sensitive information through external control agents, such as institutions, governments, or the society, who are able to apply sanctions.

From a theoretical point of view, our research identifies perceived information control as a mediator between control agents and privacy. This research extends the existing literature on control by identifying a third dimension, which considers external control agents in addition to the controller. Our findings illuminate the way in which control agents influence cloud customers during decision-making. From a managerial point of view, our study contributes to a better understanding of effective control agents acted within a cloud environment.

7.7 Acknowledgements

This research is a part of the research project, Next Generation Certification (NGCert) (www.ngcert.eu), and was funded by the German Federal Ministry for Education and Research (grant. No. 16KIS0078). The authors would like to thank dii and Wilfried Heinrich for supporting the data collection process.

8 The Formation of Perceived Privacy in Two Cultures

Title	Direct Control, Institutional Control, the Power of the Market Place and Perceived Privacy: An investigation of Cloud Sourcing Projects Across Two Cultures
Authors	Lang, Michael* (michael.lang@in.tum.de) Wiesche, Manuel* (wiesche@in.tum.de) Krcmar, Helmut* (krcmar@in.tum.de) *Technische Universität München, Chair for Information Systems, Boltzmannstraße 3, 85748 Garching, Germany
Publication	European Journal of Information Systems (EJIS)
Status	Under Review (first round)
Contribution of First Author	Problem Definition, Research Design, Data Analysis, Interpretation, Reporting

Table 29. Fact Sheet Publication P5

Abstract

Concerns about privacy risks often inhibit cloud adoption in cloud sourcing projects. To mitigate privacy risks, decision makers use different control mechanisms; namely, direct control, institutional control, and the power of the marketplace. However, cultural context, such as a client's tendency to avoid uncertainty, affects exposure to risks and the selection of control mechanisms. We find cultural differences in the mechanisms used to manage risks when choosing a cloud service provider. Clients from low uncertainty avoidance cultures rely more on their own competence to form privacy perceptions. By contrast, clients from high uncertainty avoidance cultures tend to rely more on the power of the marketplace to form their privacy perceptions. Surprisingly, institutional controls affect decision makers' perceived privacy across all cultures. This is the first study to investigate the cross-cultural formation of perceived privacy during the selection of cloud service provider in cloud sourcing projects.

8.1 Introduction

According to the industry report “Treacherous 12”, the most important cloud threat is a data breach in which sensitive business information is stolen or used in an unauthorized or unintended way (CSA 2016). As an example, Verizon, AT&T, and Sprint misused customers’ location information by sharing this information with third parties for commercial purposes. Most companies have rather realistic privacy concerns since it is no longer a matter of whether they will be attacked, but rather when they will be attacked (CSA 2016).

Cloud sourcing is an extreme form of information technology outsourcing (ITO). ITO facilitates, for example, business processes or software development. Under facilities management outsourcing a provider could be responsible for virtually all hardware and for support functions like operations and a help desk. However, a provider seldom contemplates outsourcing virtually everything (infrastructure, development platforms, security and backup, or software development) to a single party. In a cloud sourcing relationship, infrastructure, platforms, and software operations are transferred to a single cloud service provider (CSP), which induces privacy concerns (Benlian/Hess 2011).

Privacy concerns regarding the theft of intellectual property, proprietary software, or sensitive business data serve as a major inhibitor in cloud sourcing projects (Benlian/Hess 2011). Such privacy concerns in cloud sourcing are associated with the strategic risks of shirking and poaching in ITO (Clemons/Hitt 2004). Shirking involves the lack of effort to protect data because the vendor has alternative uses for the same resources (Clemons/Hitt 2004). Poaching entails a second, parallel effort of a CSP that results in a second, unauthorized revenue stream derived from data provided as a legitimate part of the contract with the client (Clemons/Hitt 2004). Clients use control mechanisms to mitigate privacy risks.

Control mechanisms are direct control, institutional control, and the power of the marketplace. In direct control, clients negotiate privacy policies, inspect technology to determine its effectiveness, or use self-deployed technologies (e.g. data encryption) to keep information private. In institutional control, clients rely on laws or certificates and expect that a third party operates according to a contract or is punished by the appropriate authorities for breach of trust. If a third party violates privacy rules, then the power of the marketplace enforces damages on the reputational capital of the company.

Risk-taking theory suggests that risk perception of clients’ decision makers affects their risk mitigation behaviour (Sitkin/Pablo 1992) and, therefore, the deployment and selection of control mechanisms. Risk perceptions are influenced by the cultural factor uncertainty avoidance, defined as the extent to which people of a culture feel threatened by unknown situations (Keil et al. 2000). Uncertainty avoidance differs among decision makers and affects what control mechanisms decision makers prefer.

Considering different uncertainty avoidance attitudes across cultures, this research investigates cloud-projects and analyses how clients mitigate privacy risks using three control mechanisms: direct control mechanisms, institutional controls, and the power of the marketplace. To do so, we conducted a cloud survey in both high and low uncertainty avoidance cultures and examined decision makers' perceived information control and perceived privacy. Our results show that high uncertainty avoidance cultures prefer direct control while low uncertainty avoidance cultures prefer the power of the marketplace during cloud sourcing decisions. Even if we expected differences in the effectiveness of institutional controls on the formation of perceived privacy within different cultures, our research indicates that institutional controls have a universal strong effect on clients' formation of perceived privacy.

8.2 Literature Review

8.2.1 Information privacy and privacy risks in cloud sourcing projects

Information privacy refers to the concept of controlling how sensitive business information is acquired and used (Pavlou 2011). Privacy has been exhaustively studied since 1945 and the privacy concept followed the evolution of information technology (Westin 2003). Between 1945 and 1960, limited information technology developments evolved decision makers' high trust in the business sector and general comfort with information collection and is defined as a baseline for the concept privacy (Pavlou 2011). After this time, privacy ran through three eras (1961–1979; 1980–199; and 1990–present) in which emerging technologies (mass production, rise of computer and network systems, and rise of the internet and related technologies, respectively) shaped the concept privacy (Pavlou 2011).

A major development in the third era, for example the rise of cloud computing, was the globalization of the privacy issue driven by rising dependencies on third parties (Westin 2003). Clients use global resources (hardware, platforms, or applications) on-demand across the globe to gain advantages such as decreasing costs (Schneider/Sunyaev 2016). However, an information asymmetry exists between decision makers who are responsible for clients' decisions and technology providers who implement privacy control mechanisms. The cause of this asymmetry is the power of the provider who possesses superior information about their capabilities and willingness to keep sensitive information private or appropriate a surplus value. After the maturity of the ITO market increased, privacy risks decreased (Schermann et al. 2016). Nevertheless, the cloud sourcing market is still an emerging market in which decision makers face privacy risks like the risk of shirking and poaching (CSA 2016).

ITO literature suggests that shirking and poaching are strategic risks since they are caused by actions that providers may initiate deliberately as part of a profit-maximizing strategy (Clemons/Hitt 2004). As cloud sourcing involves the possibility and risk of shirking and poaching tremendously increases due to the large volume of worldwide data exchange, storage, and processing possibilities of information. Should shirking or poaching occur, the existing information asymmetry prohibits a client from knowing or being able to identify the source of the superior information in the possession of the third party. Shirking and poaching do not necessarily immediately harm the client, but can embarrass them and cause a longer-term effect by damaging reputational capital. Hence, the detection of these privacy risks is difficult.

8.2.2 Perceived privacy and control perceptions

Clients use control mechanisms in cloud sourcing projects to ensure privacy. The transaction cost economics theory and agency theory are among the most commonly adopted theoretical foundations in ITO risk research (Su et al. 2014). These theories are helpful for understanding the choice of control mechanisms (Su et al. 2014). In cloud sourcing projects, clients rely on control mechanisms to assure privacy-related outcomes (Dinev et al. 2013).

Perceived control is more likely to influence a client's behaviour rather than actual control. In psychology, the construct of control has been treated as a perceptual construct because it is of greater interest than actual control when predicting behaviour (Skinner 1996). The conceptualization of perceived control is therefore a cognitive construct, and as such it may be subjective based on available information. Perceived control refers to a decision makers' beliefs regarding his or her ability to effect changes in the environment in a desired direction (Smith et al. 2011).

Perceived control influences decision makers' perceived privacy. Privacy enhancing features can provide decision makers with the means to control the disclosure, access, and use of sensitive information and, thus, increase the level of perceived control (Xu et al. 2012b). Decision makers tend to have higher privacy perceptions when they believe they have a higher level of control over the disclosure and subsequent use of their organization's information in a specific situation (Dinev et al. 2013). Hence, perceived control over information determines decision makers' level of perceived privacy.

8.2.3 Control mechanisms mitigate privacy risks

Clients try to assess and to control sensitive information based on three control mechanisms to mitigate privacy risks: direct control, institutional control, and the power of the marketplace.

Direct control aims to mitigate privacy risks through technology- and non-technology-based mechanisms and control outcomes from a clients' perspective (Culnan/Bies 2003; Son/Kim 2008). Decision makers have the possibility of using privacy-enhancing technologies, such as user identification, authentication systems, or security features (e.g., SSL connections or access management). As a result, decision makers are able to configure a preferred level of security to protect sensitive information (Xu et al. 2012b). Non-technological control enactments include mechanisms such as privacy policies provided by the CSP (Xu et al. 2011). These mechanisms provide a means by which decision makers can be informed about and/or negotiate the choices available for the way CSPs use collected information.

People experience greater autonomy when they exercise direct control (Yamaguchi 2001; Xu et al. 2012b). Such control empowers clients with mutual control over how their sensitive data and information may be used by CSPs (Xu et al. 2012b; Yamagishi/Yamagishi 1994). By using direct control, clients induce the partner to take a certain course of action with the use of strategies such as "tit-for-tat" (Axelrod/Hamilton 1981; Xu et al. 2011). By using direct control, clients match their organizational behaviours to those displayed by direct control mechanisms (e.g. cooperating versus competing) (Axelrod/Hamilton 1981).

Institutional controls aim to indirectly control outcomes (Son/Kim 2008). Institutional controls are used from partners with few resources or low power to mitigate risks and gain control through skilful and powerful certification authorities or legislation (Bandura 2001; Yamaguchi 2001).

Third party certification is defined as a "process in which a third party formally confirms that a product, process or service conforms to a set of predefined criteria" (e.g., certification scheme) (Schneider/Sunyaev 2016). These certifications provide independent verification of a provider's trustworthiness and its ability to protect information. Knowledgeable and powerful authorities capable of enforcing external sanctions (for example, certificate termination) usually provide this independent verification when CSPs are in breach of compliance with a certification scheme.

Some countries have established legislative efforts to protect sensitive information from unintended access and usage. The legal system, therefore, is a powerful control mechanism for the exercise of social control as it ensures that offenders are punished (Yamagishi/Yamagishi 1994) and thus deters potential offenders in the case of illegal or non-compliant behaviour.

Institutional controls enable clients to access resources from third parties, such as knowledge and power, to assure privacy outcomes. Should opportunistic or non-compliant behaviour occur, these control structures can provide mechanisms of voice and recourse for the betrayed creating a strong incentive for firms to refrain from opportunistic behaviour and behave appropriately (Xu et al. 2011; Shapiro et al. 1992).

Using the *power of the marketplace*, an individual attempts to control the environment as a member of a marketplace in which the marketplace serves as an agent of control (Bandura 2001). The power of the marketplace is implemented by promulgating common values, beliefs, and philosophies within the collective (Kirsch 1997). The marketplace propagates norms and values thus creating a group of individuals who share a common ideology, who have internalized a set of values, and who are committed to the collective (Kirsch 1997). If outsiders do not adhere to those norms, the marketplace can sanction outsiders through informal mechanisms like reputational capital losses. In marketplaces, responsibility (and agency) is diffused among actors (Yamagishi/Yamagishi 1994).

Reputational capital is considered to play an important role in marketplaces to mitigate risks, since it often works as a sanction mechanism against dishonest deeds (e.g., reputation as hostage) (Shapiro et al. 1992). Organizations develop reputational capital over time for engaging in appropriate conduct. Since reputation capital is a form of economic value, organizations may refrain from misconduct because they fear possible negative consequences with respect to their reputation (Shapiro et al. 1992; Yamagishi/Yamagishi 1994). A disintegrating reputation may hamper an organization from conducting ongoing business with clients (Dibbern et al. 2008). This sanctioning role of reputational capital is one of the mechanisms used to judge privacy; it directly reduces the incentive of the owner of the reputational capital to act dishonestly or non-compliant (Yamagishi/Yamagishi 1994).

Table **30** summarizes how decision makers control for privacy in a cloud environment.

Control mechanism	Control agent	Control mechanism example
Direct control	Decision maker	Monitoring, privacy policy
Institutional control	Powerful authorities	Certification, legislation
Power of the marketplace	Marketplace	Reputation

Table 30. Control mechanisms in a cloud environment

8.2.4 The effect of cultural differences in uncertainty avoidance on perceived privacy

Risk perceptions influence individual decision makers. In a company, individuals are responsible for decision-making. Therefore, a client's decisions are likely to be shaped to some extent by the cultural background of the decision maker.

A cultural factor related to risk perceptions is uncertainty avoidance (Keil et al. 2000). A decision maker's disposition to avoid uncertainty influences perceptions and risk behaviour (Srite/Karahanna 2006). As an example, opportunistic behaviour in low uncertainty avoidance cultures is likely since they do not fear the future (Nakata/Sivakumar 1996). As a consequence, these cultures distrust other people and providers because they expect others to also initiate opportunistic behaviour and put special emphasis on their own abilities (Doney et al. 1998; Xu et al. 2012b). By contrast, high uncertainty avoidance cultures are more willing to share knowledge and are influenced by social norms (Srite/Karahanna 2006). In these cultures, decision makers expect the same behaviour from their vendor who aims to have high reputational capital. In such cultures, subjective norms contribute to reducing uncertainty and opportunism (Dinev et al. 2009; Srite/Karahanna 2006).

By taking uncertainty avoidance into consideration, this study investigates the formation of decision makers' privacy judgements within a cloud environment. Figure 12 illustrates our conceptual research model.

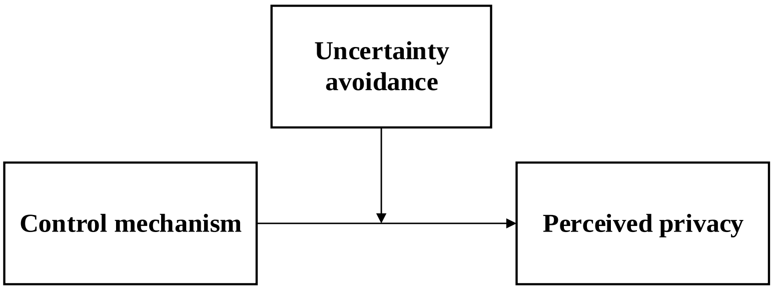


Figure 12. Conceptual research model

8.3 Hypotheses Development

Research on the formation of privacy perceptions is based on a control agency perspective (Xu et al. 2012b). In particular, this perspective allows not only an examination of the effects of direct control, institutional control, and the power of the marketplace during privacy judgements (Yamaguchi 2001), but also the influence of cultural differences on the perceived effectiveness of these controls.

Before we outline our hypotheses, we define our dependent variable perceived privacy: Perceived privacy describes the differences between an intended and actual state of privacy. Decision makers have expectations regarding collection and subsequent access, use, and disclosure of sensitive information as representative characteristics that influence their privacy perceptions (Dinev et al. 2013). Perceived privacy results when decision makers compare the actual and ideal collection and subsequent access, use, and disclosure of their sensitive business information (Chellappa 2008). Perceived privacy refers to an aggregation of decision makers' perceptions and expectations regarding a provider's characteristics (Chellappa 2008). Perceived privacy is defined as a decision makers' "self-assessed state in which external agents have limited access to information" (Smith et al. 2011).

8.3.1 Information control and perceived privacy

In accordance with previous research, we conceptualize information control as a perception and define it as being an individual's belief in the ability to determine the extent to which sensitive company information, such as sensitive information from decision makers, or sensitive information will be released within a cloud environment in an unintended way (Dinev et al. 2013). Prior literature differentiates between two types of control important in a privacy context: control over information disclosure and control over information use once the information has been obtained (Culnan/Armstrong 1999). Most commonly, providers within the internet address the first type of control by offering granular privacy settings, which limit the accessibility of sensitive information to other members and third parties. It has been suggested that individuals feel they have a higher level of privacy when they have a sense of information control (Culnan/Bies 2003). Recent studies on privacy suggest that a loss of information control is central to the perception of privacy invasion (Dinev et al. 2013). Accordingly, our hypothesis in this respect is as follows:

> ***Hypothesis 1 (H1):*** *Cloud decision makers' perceived information control positively affects perceived privacy.*

8.3.2 Cultural effects on the effectiveness of control agents

Cultural effects on direct control. Decision makers' risk perceptions are a strong influence in high uncertainty avoidance cultures, which in turn leads to a risk avoidance behaviour (Keil et al. 2000). By contrast, low uncertainty avoidance cultures are more likely to take risks and are not afraid of the future leading to a higher likelihood of opportunistic behaviour (Nakata/Sivakumar 1996). Hence, there is a tendency to distrust other people and organizations in such cultures (Doney et al. 1998). Low uncertainty avoidance cultures place special emphasis on their own abilities and common sense, and, thus, prefer self-control (Srite/Karahanna 2006). In this sense, studies identified that individuals of low uncertainty avoidance cultures trust in the behaviour of another party is mainly developed through security protection mechanisms, which reflect direct control mechanisms (Kim 2008).

Because of these relationships, we assume a moderating effect of uncertainty avoidance culture on the relationship between direct control and decision makers' information control perception as follows:

> ***Hypothesis 2 (H2):*** *Direct control mechanisms enhance cloud decision makers' perception of information control stronger for low uncertainty avoidance cultures than for high uncertainty avoidance cultures.*

Cultural effects on institutional control. Cultures with high uncertainty avoidance have a need for rules and structure, and require a high amount of verified information (Hofstede 2011; House et al. 2004). Clearly defined codes of conduct, laws, and regulations create certain and predictable outcomes for these cultures (Hofstede 2011). Studies demonstrate that a sample from Singapore (with a high uncertainty avoidance culture), have a desire for a higher degree of government regulation (Xu et al. 2012b). High uncertainty avoidance cultures prefer to rely on external third parties to gain external justification for their behaviour, for example through certification, in certain situations (Kim 2008). Our hypothesis in this respect is as follows:

> ***Hypothesis 3 (H3):*** *Institutional control mechanisms enhance cloud decision makers' perception regarding information control more strongly for high uncertainty avoidance cultures than for low uncertainty avoidance cultures.*

Cultural effects on the power of marketplaces. In cultures with high uncertainty avoidance, the focus is on eliminating as much of the uncertainty as possible in order to create certain and predictable outcomes (Srite/Karahanna 2006). In particular, in situations during which sensitive information is transferred, a high degree of uncertainty exists because of the concern about how the information is handled (Xu et al. 2012b). Some studies show that subjective norms can contribute to reducing this uncertainty through informal or normative influences (Dinev et al. 2009; Srite/Karahanna 2006). The reason for this is that the opinions of colleagues, friends, or the public provide additional information for individuals, which in turn reduces the uncertainty about a decision. In a high uncertainty avoidance culture, a person orients himself/ herself to the social environment and to what is socially acceptable and appropriate (Srite/Karahanna 2006). Thus, people in a high uncertainty avoidance culture search for an external justification, such as a good reputation, to gain control about a certain situation. Our hypothesis in this respect is as follows:

> ***Hypothesis 4 (H4):*** *The power of marketplace leads to an increased sense of perceived control over sensitive information on the part of the cloud decision maker more strongly for high uncertainty avoidance cultures than for low uncertainty avoidance cultures.*

Figure 13 shows the research model used in this study.

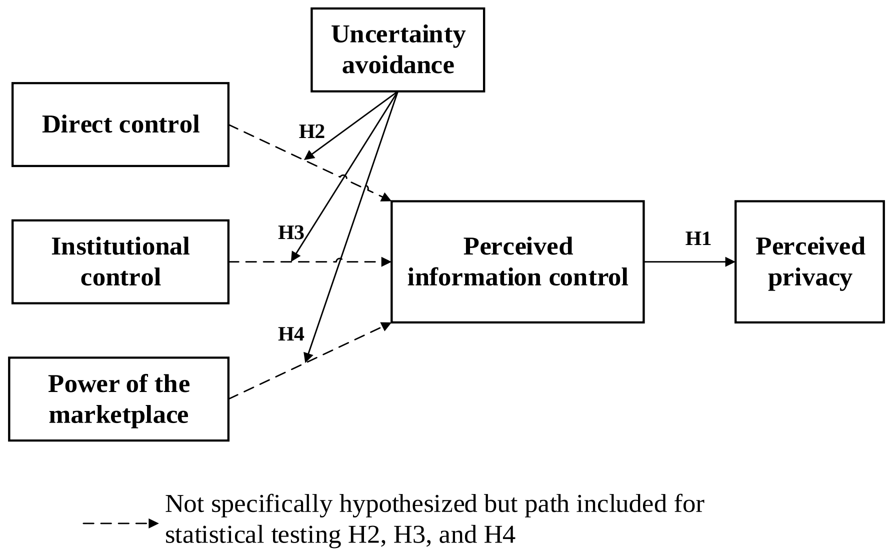

Uncertainty avoidance
Direct control
Institutional control
Power of the marketplace
Perceived information control
Perceived privacy
H1
H2
H3
H4
Not specifically hypothesized but path included for statistical testing H2, H3, and H4

Figure 13. Cloud privacy research model

8.4 Methodology and Data Collection

8.4.1 Data collection and sampling

To enable ease of design without sacrificing rigor, we conducted our research within a cloud sourcing projects environment to match our target population. We empirically tested our research hypotheses using data collected through a survey of clients from different cultures that included items for the constructs specified in the model. Hence, our moderator effect is categorical and high and low uncertainty avoidance cultures serve as a two-group construct that divides the data into two subsamples (Kim et al. 2015). We used the GLOBE-Index for the selection of high and low uncertainty avoidance cultures (House et al. 2004) since it can be used to measure differences in uncertainty avoidance attitudes within organizations (Vance et al. 2008).

We chose Germany as a high uncertainty avoidance culture, which reached a score of 5.19 on the GLOBE-Index (House et al. 2004). The high uncertainty avoidance sample of our survey was drawn from a market research company, a leading research company studying digital developments within Germany. To increase the external validity of our study, the market research company did not constrain the sample to specific industries or to firms of a specific size, and instead drew a random sample from the entire population of cloud decision makers responsible for cloud sourcing projects within their database. Overall, 5000 cloud decision makers were contacted. We received 141 valid answers representing a response rate of 3%.

Research identified that the cultural effect of two Western but culturally distinguishable nations like their tendencies to avoid uncertainty affects decision maker's privacy perception and behaviour (Dinev et al. 2006). Therefore, as a low uncertainty avoidance culture, we chose the UK and the US that reach an uncertainty avoidance score of 4.65 and 4.15 on the GLOBE-Index, respectively. These scores were significantly different from the German sample. For the low uncertainty avoidance sample of our survey, we adopted a purposive sampling strategy.

Our reason for choosing a purposive sampling technique is that professional cloud decision makers are rare and only selected subjects are suitable for our study. Therefore, based on keywords like “cloud selection”, we set up a data base consisting of cloud decision makers responsible for cloud sourcing projects within our target population drawn from the social network “LinkedIn”. We sent out our survey to 2,000 cloud decision makers and received 82 valid answers, which represents a response rate of 4%. We used t-tests to investigate the mean differences of responses between the UK and the US. No significant differences were observed.

In total, 223 usable responses from cloud sourcing projects were available for data analysis. The samples demographics and cloud sourcing project characteristics of the cloud surveys within the high and low uncertainty cultures are shown in

Table **31**.

Decision makers demographics		**Percent**		**Cloud sourcing project characteristics**		**Percent**	
		High UA	**Low UA**			**High UA**	**Low UA**
Position	CEO	20	31	Deployment model	Public	55	47
	IT Manager	49	24		Hybrid	25	27
	Business Manager	31	45		Private	20	26
Age (years)	<24	0	5	CS model	SaaS	43	51
	25-34	11	20		PaaS	26	19
	35-44	38	32		IaaS	31	30
	45-54	32	30	Cloud size	<10k €	38	28
	>55	18	13		10k-25k €	23	31
Cloud usage duration (years)	<1	37	26		>25k €	39	41
	1-3	38	36	Personal data	Yes	76	81
	>3	25	38		No	24	19

UA = uncertainty avoidance; CS = cloud service

Table 31. Decision makers’ demographics and cloud sourcing project characteristics of cloud survey within high and low uncertainty avoidance cultures

8.4.2 Survey procedure

The current study utilized a “key informants” methodology for data collection, which is a popular approach in empirical information systems studies. In organizational survey research, targeted respondents assume the role of key informants and provide information on a particular unit of analysis by reporting on project properties. However, if a respondent lacks appropriate knowledge, the results can be confusing and may lead to erroneous conclusions. Therefore, both survey questionnaires were mailed to the most senior IT executive of each firm (e.g., to the chief information officer, the vice president in charge of IT, or the vice president in charge of business) responsible for the selection of distinct cloud services along with a cover letter outlining the purpose of the research and soliciting participation.

To foster participation and reduce self-reporting bias, all participants were offered a report on their company’s position compared with that of others of a similar size and industry. A pre-test assisted us in the development of both the content and the format of specific questions presented in the survey. 20 native German speaking practitioners known by the marketing research company and 18 native English-speaking practitioners from various industries known by the research team evaluated the survey items. We also employed two further academics who are experts in cloud computing research to review both questionnaires. After minor changes in wordings, the final surveys were distributed.

8.4.3 Scale development

Scale development for the reflective constructs (Table 32) was based on an extensive survey of literature on privacy and psychological control. We adapted validated standard scales and constructs for our use as far as possible. All questions (except those regarding legislation) were answered using a Likert scale ranging from 1 to 5, with 1 representing the lowest score as “completely disagree” and 5 representing the highest score as “completely agree”. Legislation questions were answered using a Likert scale ranging from 1 to 5 as well but with 1 representing the lowest score as “very low” and 5 representing the highest score as “very high” on the item scale.

Direct control and institutional control have the two dimensions privacy policy and privacy enhancing technology, and legislation and certification, respectively (Table 32). The sub-dimensions can be viewed as causing the focal construct and are not interchangeable. Accordingly, we operationalize direct control and institutional control as formative, second-order construct composed of two, first-order reflective constructs (Polites et al. 2012).

Construct		Reflective measurement	Loading High UA*	Loading Low UA*	Source
Perceived Privacy (PRI)					Dinev et al. (2013)
		Our company feels it has sufficient privacy when using this cloud service.	0.94	0.93	
		Our company is comfortable with the amount of privacy it has.	0.94	0.93	
		Our company thinks its privacy is preserved when using this cloud service.	0.95	0.94	
Perceived Information Control (PIC)					Xu et al. (2011)
		I believe our company has control over who can get access to our sensitive information collected by this cloud service provider	0.94	0.92	
		I think our company has control over what sensitive information is released by this cloud service provider.	0.94	0.94	
		I believe our company has control over how sensitive information is used by this cloud service provider.	0.95	0.91	
		I believe our company can control its sensitive information provided to this cloud service provider	0.96	0.94	
Direct control	Privacy Policy (PP)				Xu et al. (2011)
		Our company feels confident that this cloud service provider's privacy statement reflects a commitment to protect our data.	0.90	0.94	
		With its privacy statement, our company believes that our personal information will be kept private and confidential by this cloud service provider.	0.93	0.95	
		Our company believes that this cloud service provider's privacy statement is an effective way to demonstrate its commitments to privacy.	0.83	0.91	
	Privacy enhancing technology (PET)				Hossain/Prybutok (2008)
		For our company, computer and network security is extremely important when dealing with this cloud service.	0.89	0.74	
		For our company, user identification and authentication are extremely important when dealing with this cloud service.	0.90	0.78	
		For our company, security features (such as SSL connections) are extremely important when dealing with this cloud service.	0.91	0.76	
		For our company, client and server security are extremely important when dealing with this cloud service.	0.86	0.83	
Institutional control	Legislation (LEG)				Koh et al. (2012)
		How confident are you with the legal system in the cloud service provider's country?	0.77	0.70	
		In your opinion, how effective are the laws and regulations in the supplier's country concerning the following activities?			
		• Governing operations and transactions of the cloud service provider	0.87	0.91	
		• Resolving legal disputes	0.91	0.89	
		• Ensuring data privacy in the cloud	0.90	0.92	Self-developed
		• Ensuring data security in the cloud	0.78	0.89	
	Certification (CER)				Kim et al. (2015)
		The presence of a privacy certification of this cloud service provider makes our company feel more comfortable.	0.95	0.92	
		The presence of a privacy certification of this cloud service provider makes our company feel safer in terms of privacy.	0.95	0.93	
		The presence of a privacy certification of this cloud service provider makes our company feel safer in terms of security.	0.91	0.91	
		When our company purchases cloud services, the privacy certification of the cloud service provider for privacy assurance by independent institutions are important to us.	0.86	0.86	
Power of the	Reputation (REP)				Doney/Cannon (1997)
		This cloud service provider has a reputation for being honest.	0.92	0.89	
		This cloud service provider is known to be concerned about its clients. **	0.65	0.76	
		This cloud service provider has a high reputation on the market.	0.92	0.94	

* Factor loadings are significant at the p<0.001 level
** Item was dropped
UA= uncertainty avoidance

Table 32. Operationalization of the constructs

Several control variables were added to control for the results affected by extraneous factors. These included participants' experience of cloud sourcing, the deployment model used by a specific cloud service, and whether personal data from customers are processed within this specific cloud service.

To avoid potential language-barrier problems, the survey within Germany was provided in German. However, to check for translation bias within measurement items, a back-translation technique was employed whereby two different translators translated the German questionnaire back into English. The back-translated items had a high degree of correlation with the original English items, thereby assuring a relative lack of translation bias.

8.4.4 Measurement model testing

We adopted constructs used in previous studies to assure validity of the constructs used. Our measurement model was validated using the standard procedure of Straub (1989), and to assess the convergent and discriminant validity of items, the items of the scale were pooled into a related domain. While convergent validity was determined both at the individual indicator level and at the specified construct level, discriminant validity was assessed by analysing the average variance extracted and inter-construct correlations.

Results showed that all the factor loadings were significant, suggesting convergent validity (Table 32). All constructs met the threshold value for the average variance extracted (AVE>0.50) and Cronbach's alpha (alpha>0.70), as suggested by Straub (1989) (Table 33 and 34). For the discriminant validity of latent variables, the square roots of AVEs exceeded inter-construct correlations that were negligibly low between independent constructs. In addition, composite reliability (CR) was calculated and evaluated for each construct; all constructs were found to have a CR that was significantly above the cut-off value of 0.70. In summary, the quality of the measurement models was proven to be satisfactory.

	Mean (Std)	alpha	CR	AVE	PRI	PIC	PP	PET	LEG	CER	REP
PRI	3.89 (1.03)	0.93	0.95	0.87	0.94						
PIC	3.35 (1.33)	0.95	0.96	0.87	0.64	0.94					
PP	3.84 (1.08)	0.92	0.86	0.87	0.61	0.55	0.89				
PET	4.39 (0.83)	0.93	0.91	0.82	0.27	0.20	0.28	0.89			
LEG	3.54 (1.18)	0.92	0.90	0.75	0.59	0.61	0.54	0.35	0.85		
CER	3.61 (1.18)	0.93	0.94	0.83	0.42	0.36	0.57	0.58	0.39	0.92	
REP	4.23 (0.81)	0.80	0.82	0.83	0.60	0.53	0.55	0.28	0.52	0.38	0.92

Table 33. Assessment of measurement model for high uncertainty avoidance cultures

	Mean (Std)	alpha	CR	AVE	PRI	PIC	PP	PET	LEG	CER	REP
PRI	4.04 (0.93)	0.93	0.96	0.89	0.93						
PIC	3.87 (1.09)	0.96	0.97	0.89	0.71	0.94					
PP	4.07 (0.86)	0.86	0.92	0.79	0.63	0.69	0.93				
PET	4.34 (0.98)	0.91	0.94	0.80	0.28	0.43	0.42	0.91			
LEG	3.76 (1.05)	0.90	0.93	0.72	0.61	0.50	0.54	0.38	0.87		
CER	3.98 (0.99)	0.94	0.96	0.84	0.29	0.50	0.59	0.43	0.45	0.91	
REP	4.25 (0.77)	0.82	0.92	0.85	0.42	0.35	0.42	0.49	0.33	0.25	0.91

Table 34. Assessment of measurement model for low uncertainty avoidance cultures

For the second-order formative constructs direct control and institutional control, significance of dimension weights was examined to determine the relative contribution of items to the construct (Polites et al. 2012). All dimensions were significant at p<0.001, indicating satisfactory validity.

8.5 Results

8.5.1 Structural model testing

We used SmartPLS 3.2.7 to validate the structural models and to test the hypotheses using the bootstrapping (1000 resamples) method. The second-order direct control and institutional control constructs were estimated using the factor scores of their first-order dimensions as formative indicators (Polites et al. 2012). Figure 14 summarize the results of the two structural models for high and low uncertainty avoidance cultures.

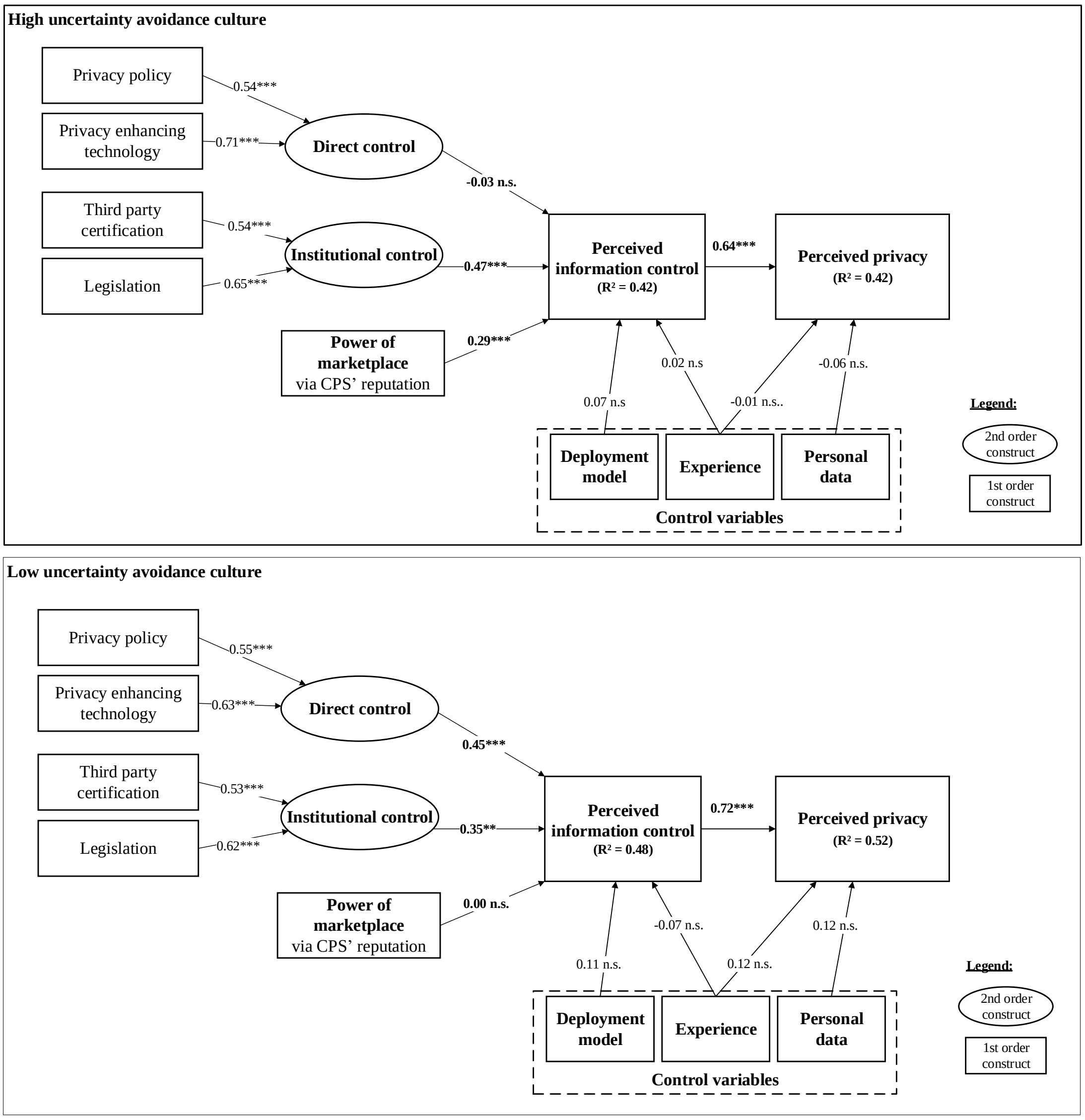


Figure 14. Results for high and low uncertainty avoidance cultures for cloud privacy structural models

H1 is supported. For the relationship between perceived information control and perceived privacy, Figure 14 demonstrates for high uncertainty avoidance countries a path coefficient=0.64 and p<0.001 and for low uncertainty avoidance countries a path coefficient=0.72 and p<0.001.

In both samples, none of the control variables had a significant effect on perceived information control or perceived privacy.

8.5.2 Group comparison analysis

We tested the moderating effect of a client's culture by conducting a multiple group analysis. Thus, differences between the path coefficients of our two samples (high and low uncertainty avoidance cultures) are tested for significance with pair-wise t-tests (Table 35).

Independent Variable	**Dependent Variable**	**High UA n=141**		**Low UA n=82**		**Sample Differences**	
		Path	**P-value**	**Path**	**P-value**	**Path**	**P-value**
Direct control	Perceived information control	-0.03	0.25	**0.45**	**<0.001**	**0.48**	**<0.001**
Institutional control	Perceived information control	**0.47**	**<0.001**	**0.35**	**<0.001**	0.12	0.21
Power of the marketplace	Perceived information control	**0.29**	**<0.001**	0.00	0.94	**0.29**	**0.04**

UA= uncertainty avoidance

Table 35. Cloud privacy results for structural model and group comparison

H2 is supported. For the group comparison between high and low uncertainty avoidance cultures, we found the path coefficient=0.48 and p<0.001.

H3 is not supported. For the group comparison between high and low uncertainty avoidance cultures, the path coefficient=0.12 and p>0.05.

H4 is supported. For the group comparison between high and low uncertainty avoidance cultures, the path coefficient=0.29 and p<0.05.

8.6 Discussion

8.6.1 Findings

Our research demonstrates that clients in high uncertainty avoidance cultures prefer institutional control and the power of the marketplace to increase their perceived information control and perceived privacy. By contrast, clients in low uncertainty avoidance cultures prefer direct control and institutional control to increase their perceived information control and perceived privacy. We show that the power of the marketplace has a significant higher effect in high uncertainty avoidance cultures compared to low uncertainty avoidance cultures. Direct control has a significantly higher effect in low uncertainty avoidance cultures compared to high uncertainty avoidance cultures.

8.6.2 Theoretical implications

Our results demonstrate the influence of three control agents, direct control, institutional control, and the power of the marketplace, on a client’s perceived control over information in different cultures. Subsequently, perceived control over information influences a client’s perceived privacy in cloud sourcing projects.

We contribute to literature by demonstrating how different cultures use different control mechanisms to mitigate privacy risks, and, therefore, increase perceived privacy. Srite/Karahanna (2006) found that decision makers from high uncertainty avoidance cultures are influenced more by their peers to determine whether they should use the technology than are low uncertainty avoidance decision makers. By contrast, Xu et al. (2012b) identified that decision makers of low uncertainty avoidance cultures are influenced by direct controls to form their control and privacy perceptions. Our results demonstrate that both findings are in line: We show that decision makers from low uncertainty avoidance cultures rely more on their own competence to form privacy perceptions and high uncertainty avoidance cultures tend to rely more on the power of the marketplace (therefore, inter-personal, non-technical) mechanisms to form their privacy perceptions.

These findings are important for research conducted in multi-national organizations buying and selling services across the globe. Research has to consider cultural differences of clients and related preferences on control mechanisms to mitigate privacy risks in cloud sourcing projects. While our study was conducted in cloud sourcing projects, these findings might also provide first explanations about how cultural differences influence individual customers in decision making in an online environment.

Our results also inform research using a design perspective on control mechanisms in different cultures. Depending on the culture in place, research should use different design artefacts. While the power of the market can be employed, for example, using recommendation systems, direct control mechanisms require interactions from the decision maker. Therefore, while multiple control artefacts might be available, the culture in place provides a first selection criterion to assure successful design artefacts.

Our results do not support the notion that institutional control influences a client’s perceived information control and perceived privacy of high uncertainty avoidance countries significant higher than of low uncertainty avoidance countries.

We explain these findings based on the existing information asymmetry between CSP and clients. Institutional controls are powerful mechanisms with low transaction costs for the client (Kim 2008; Xu et al. 2011). While direct control requires a higher effort from the client, by using the power of the marketplace clients rely on unknown external control agents. Therefore, by having a powerful, well-known institutional control agent like the government or a certification authority, clients across the globe are able to gain perceived control and privacy over their sensitive information to mitigate privacy risks such as shirking and poaching.

We contribute to literature by demonstrating the influence of control mechanisms on a client’s control and privacy perceptions to mitigate privacy risks. Research identified that direct and institutional control influences a client's control perceptions and, subsequently, privacy concerns (Xu et al. 2012b). While privacy concerns are associated with negative feelings and can be used just as a proxy for privacy (Dinev et al. 2013), perceived privacy measures a client's perceptions directly without negatively influencing them. We extend these findings by (1) demonstrating that in addition to direct control and institutional control, also the power of the marketplace – therefore social and normative influences – is important to influence control perceptions, and (2) control perceptions influence perceived privacy per se in cloud sourcing projects.

Such findings are important for research that investigates ITO projects. In addition to well-studied direct controls and institutional control mechanisms (Xu et al. 2012b; Kirsch 1997), research should consider social and transparency building aspects during professional decision making.

Furthermore, our findings implicate that privacy is a multi-dimensional construct highly influenced by privacy control mechanisms. Information privacy is a multi-dimensional variable that refers to the concept of controlling how sensitive business information is acquired and used (Pavlou 2011). Direct control, institutional control, and the power of marketplace are used to mitigate the risk of shirking and poaching. As our findings explain the variance of perceived privacy to 42%, privacy control mechanisms are essential to form a client's perceived privacy.

8.6.3 Managerial implications

From a practitioner's perspective, we contribute to clients, CSPs, legislative and certification authorities, and the society as a whole by determining effective control mechanisms that influence clients of different cultures in a cloud environment.

Our results assist clients and responsible cloud decision makers in identifying appropriate control mechanisms to assure that a CSP has adequate security and privacy protection in place. For CSPs, our results indicate which control mechanisms are appropriate for use in protecting privacy from a client's perspective in different cultures. Our findings also provide responsible governments, certification authorities, and society with feedback on the effectiveness of their endorsements. These groups might use our results to improve their services and employ reliable and reputable certification authorities, or to consider further channels to share opinions and information on the reputation of service providers.

8.6.4 Limitations and future research

In this study, we use a comparative approach to investigate the moderating effect of high and low uncertainty cultures on a client's control agent choice. Therefore, in line with other studies on culture, this study is based on the assumption that our sample including data from the UK, US, and Germany represents two different uncertainty avoidance cultures; people belonging to a single cultural group and a national cultural group are static, homogeneous, and mutually exclusive (Keil et al. 2000). Even if the culture to which the client belongs highly influences his/her behaviour (House et al. 2004), individual differences in his/her tendency to avoid uncertainty are likely. Future research could address this limitation by considering cultural values as an individual factor when studying the impact of culture on certain IT outcomes and including these individual factors as an independent construct.

The focus of this study was experienced decision makers in a cloud environment. We selected this population because if a respondent lacks appropriate knowledge on cloud sourcing projects, the results can be confusing and may lead to erroneous conclusions. The formation of a client's privacy perception without experience within a cloud environment could differ from the perceptions of a client with extensive experience. Future research can take this into consideration by providing a comparison between unexperienced and experienced clients during cloud decision making.

8.7 Conclusion

The conduct of this study was motivated by the notion of a national context such as a client's tendency to avoid uncertainty can affect the client's exposure to risks and his/her preferences for control mechanisms. We found that clients use different mechanisms in each country to manage risks when choosing their cloud service provider. Clients from low uncertainty avoidance cultures rely more on their own competence to form privacy perceptions. By contrast, clients from high uncertainty avoidance cultures tend to rely more on the power of the marketplace to form their privacy perceptions. Surprisingly, institutional controls affect decision-makers' perceived privacy across all countries. These results can help researchers and clients in different cultures to better understand the formation of privacy perceptions.

9 Impact of Cloud Assurance Seals on Customers’ Perceived Privacy

Title	Explaining the Impact of Cloud Assurance Seals on Customers’ Perceived Privacy
Authors	Lang, Michael* (michael.lang@in.tum.de) Wiesche, Manuel* (wiesche@in.tum.de) Krcmar, Helmut* (krcmar@in.tum.de) *Technische Universität München, Chair for Information Systems, Boltzmannstraße 3, 85748 Garching, Germany
Publication	European Conference on Information Systems (ECIS)
Status	Accepted
Contribution of First Author	Problem Definition, Research Design, Data Analysis, Interpretation, Reporting

Table 36. Fact Sheet Publication P6

Abstract

Privacy concerns inhabit professional cloud adoption. Assurance seals resulting from a third-party certification are frequently used from cloud service provider to provide privacy assurance for their customers. However, empirical findings on the effectiveness of assurance seals focusing on “who” issues those, even if customers also require the information why the assurance seal is valid and reliable. To fill this gap, we build on information integration theory and investigate the impact of certification authorities’ reputation and the quality level of an audit on customers’ perceived privacy within a professional cloud environment by using an experimental design including 43 professional cloud decision makers. We show that certification authorities’ reputation does not alone produce opinion change, it rather affects customers’ perceived privacy resulting from the quality level of an audit. Our findings have theoretical implications for the information integration theory and assurance seal research. We also discuss the managerial implications of our work for cloud service providers and certification authorities.

9.1 Introduction

Privacy concerns remain a major inhabiting factor for the adoption of cloud services (Schneider/Sunyaev 2016). To reduce privacy concerns, cloud service providers (CSPs) use audits to certify their products, processes or services through an independent authority and illustrate the results using assurance seals (Oezpolat et al. 2013; Lang et al. 2018b). Assurance seals decrease concerns of customers by providing the information as to which independent authority (e.g. certification authority) is providing assurance (e.g. privacy assurance) (Kimery/McCord 2002a; Lang et al. 2018a). As an example, the TÜV as a certification authority can certify according to the ISO 27001 standard that a CSP has a security management system that assures confidential, reliable, and secure treatment of customers' data and ordered services.

Research has frequently investigated the effectiveness of assurance seals. Several studies have identified a significant positive impact of assurance seals in terms of achieving their intended effects like reducing privacy concerns on digital services (Xu et al. 2012b). Various other studies have been unable to confirm a significant impact of assurance seals in terms of achieving their intended effects like the improvement of location-based service selection behaviour (Keith et al. 2015) or the influence of consumers' perceived privacy risk (Xu et al. 2011). Hence, despite the popularity of assurance seals, research would benefit from a better understanding of what determines the effectiveness of assurance seals in an online environment (Oezpolat et al. 2013; Lowry et al. 2012).

Information integration theory explains why assurance seals' source and scope determine its effectiveness. The effectiveness of assurance seals describes the degree to which a certification achieves its intended effects (e.g. increasing perceived privacy) (Lins/Sunyaev 2017). Information integration theory provides the framework for cognitive evaluation and the integration of information, e.g. from assurance seals (Sethi/King 1999). Each item of information is determined by its weight (relative importance of an item of information) and scale value (semantic properties of an item of information) (Sethi/King 1999; Lowry et al. 2008). While customers integrate assurance seals' source reputation to influence their overall perception (Lowry et al. 2008), the assurance seals' scope (e.g. privacy) must match the related concerns (e.g. privacy concerns) and determine the altitude (positive or negative) of an overall perception regarding an online service (Kim et al. 2015; Kimery/McCord 2002a). Therefore, research found two determinants – (1) third-parties' reputation and (2) the scope of an assurance seal – of the effectiveness of assurance seals.

To form privacy perceptions of customers regarding an online service effectively, customers also require, along with the source, information about the validity and reliability of the privacy assurance seals. Online services like cloud services are an ever-changing environment (Lins et al. 2016). Assurance seals' validity and reliability vary because of different levels of audit qualities (Oezpolat et al. 2013). While some assurance seals result from an in-depth or even continuous certification process, others only confirm that an online retailer has existed at the time of certification (Oezpolat et al. 2013). From trust-assuring arguments, we know they are most effective when customers receive reasons for why the argument is valid (Kim/Benbasat 2006). As customers are able to differentiate between privacy assurance seals (Moores 2005), we assume the validity and reliability of assurance seals determine their effectiveness to form privacy perceptions.

This paper addresses this gap and investigates how the source reputation and information about assurance seals' validity and reliability determines the effectiveness of privacy assurance seals. We build on the information integration theory (Anderson 1981) and investigate the impact of certification authorities' reputation and the quality level of the audit process on customers' perceived privacy within a professional cloud environment. We show that certification authorities' reputation does not alone produce a change of opinion (Lowry et al. 2008), rather it affects customers' perceived privacy resulting from the quality level of the audit process.

To do this, we first outline the theoretical foundation of the information integration theory and develop the logic underlying the research hypotheses. Second, we present the research methodology and results. The paper concludes with a discussion of the key findings, direction for future research, theoretical contribution and managerial implications of the results.

9.2 Theoretical background and hypotheses

9.2.1 Information integration theory

The information integration theory explains the cognitive integration of available information and addresses the question as to how people derive an overall attitudinal disposition from an array of knowledge and beliefs they hold about an attitude object (Anderson 1981). For the cognitive integration of available information, two concepts are important: valuation and integration (Sethi/King 1999).

Valuation refers to the process of determining the evaluative scale values and weights assigned to each item of information that contributes to attitudinal judgment. The weight parameter reflects the influence of the cognitive element in determining the overall attitude and can vary from zero to one with its value influenced by the context (Sethi/King 1999). As an example, individuals weigh the importance of an item of information by the sources' reputation (Anderson 1971). The scale value reflects semantic properties, varies from positive to negative and is considered independent of context and other cognitive elements (Sethi/King 1999). As an example, the good or bad actions of presidents of the United States influenced their favorability and people's election behavior (Anderson 1974).

Integration refers to the process of combining the information units into an overall attitudinal judgment. Individuals combine the weight and scale value parameters into a single judgment (Anderson 1974). In this way, a weight parameter does not itself produce a change of opinion, but affects the degree of the stimulus resulting from the scale value of an item of information (Anderson 1971).

The information integration theory is particularly useful in understanding the effects of assurance seals on information system customers. Simonin/Ruth (1998) demonstrate positive spill-over effects of highly reputable partners on lower reputable partners in a brand alliance. Lowry et al. (2008) extend such a finding by also demonstrating positive spill-over effects of brand seal from a highly reputable third-party on an unknown website. Both show how preexisting impressions of an association with a known third-party combined with an unknown organization or website create an overall (positive or negative) impression (Lowry et al. 2008).

Assurance seals have different semantic properties and beside the weight parameter (e.g. certification authorities' reputation), the scale value is particularly important in determining the effectiveness of assurance seals. Kim/Benbasat (2006) identified that arguments consisting of the semantic properties as to what (assurance seals' scope) is assured and the reasons for why customers should rely on this information are most effective in influencing customers' perceptions. However, in contrast to Kim/Benbasat (2006), the source of the assurance seal is not the counterpart itself, instead the source is an independent third-party that is even more effective in influencing customers' perceptions (Kim/Benbasat 2009). Therefore, in addition to the semantic properties, customers weigh the available information because of its personal relevance (Anderson 1981).

To determine the CSPs' ability to protect privacy through assurance seals, customers integrate the available information about the certification authorities' reputation (source) and the quality level of an audit (validity and reliability) (similar to "weights" and "scale value" in information integration theory) into their information processing to form an overall perception about the CSP (Anderson 1981; Simonin/Ruth 1998). Certification authorities' reputation influences the personal relevance of the information (Lowry et al. 2008; Anderson 1971). In line with Anderson (1974), the quality level of an audit determines the scale value to protect privacy. To understand how different degrees of the effectiveness of assurance seals occur, it is important to consider both dimensions (weight and scale value).

9.2.2 Customers' privacy perceptions and assurance seals in a cloud environment

9.2.2.1 Perceived privacy in an online environment

In an online environment, a perceived state of privacy (short perceived privacy) refers to an aggregation of consumers' perceptions and expectations regarding a provider's characteristics when storing or processing sensitive information (Chellappa 2008; Frye/Dornisch 2010). A group of scholars (Bansal et al. 2015; Smith et al. 1996) includes customers' perceptions regarding collection and subsequent access, use, and disclosure of sensitive information as representative characteristics that influence one's privacy perceptions. Collection refers to what sensitive information a provider collects from a customer. Access refers to whether or not reasonable steps are in place to assure that sensitive information is accurate and secure from unauthorized use. Use refers to whether or not sensitive information will be used for purposes other than those for which they have been provided. Disclose refers to whether or not sensitive information is disclosed to secondary parties. Perceived privacy results when consumers compare the actual and expected collection and subsequent access, use, and disclosure of their sensitive information (Chellappa 2008; Frye/Dornisch 2010).

Therefore, perceived privacy reflects the amount of consumers' belief that the institutional setup allows for the privacy of their transaction to be maintained as promised. Perceived privacy is defined as "an individual's self-assessed state in which external agents have limited access to information" (Smith et al. 2011).

9.2.2.2 Privacy assurance seals in a cloud environment

Cloud computing "is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources" (Mell/Grance 2011). Customers use these resources to process, transfer, and store sensitive information, such as personal data from their customers, and to gain advantages with respect to costs and flexibility (Mell/Grance 2011; Böhm et al. 2010). However, existing information asymmetry between the customer and the CSP and resulting privacy concerns serve as major inhibitors in adopting cloud services.

To overcome privacy concerns, customers seek an independent third-party certification and resulting assurance seals to assure privacy when adopting cloud services (Yang/Tate 2012; Lang et al. 2017, 2016). Privacy assurance seals inform (potential) customers of a CSP in three dimensions (Lansing et al. 2018): First, whether the provider complies with the certification scope. Second, information about the certification process itself. Third, the issuers brand of the assurance seal.

To obtain an assurance seal, a CSP typically goes through a certification process administered by a certification authority. Such certification processes include an audit to verify the quality specification from the certification scope, for instance, contractual requirements (e.g. service level agreements), legal requirements (e.g. privacy policy), security requirements (e.g. encryption), business processes (e.g. data protection management), and data center infrastructure (e.g. physical access control) (Sunyaev/Schneider 2013). Depending on the audit process, static versus continuous, an audit takes place typically every third year or continuously, respectively (Anisetti et al. 2017; Lins et al. 2016). Upon successful completion of this process, the CSP is permitted to display the assurance seal and an attestation report on its website.

Figure 15 summarizes the involved roles and interactions to obtain an assurance seal from the certification authority.

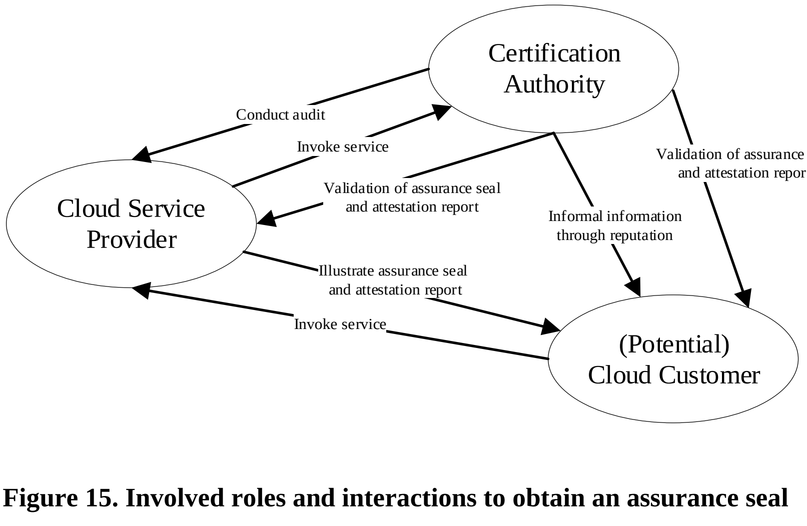

Certification Authority
Conduct audit
Invoke service
Validation of assurance seal and attestation report
Cloud Service Provider
Validation of assurance seal and attestation report
Informal information through reputation
Illustrate assurance seal and attestation report
Invoke service
(Potential) Cloud Customer

Figure 15. Involved roles and interactions to obtain an assurance seal

9.2.2.3 Source of an assurance seal

In a professional service engagement, e.g. cloud service certification, customers do not enjoy perfect information to determine a service quality (Shaked/Sutton 1982). As a result of imperfect information, customers frequently rely on companies' reputation as a surrogate measure of quality (Barzel 1982). As it is expensive and takes a long period of time for certification authorities to build a high reputation, certification authorities avoid verification or attestation services that do not meet the communicated privacy requirements (Zhao et al. 2009; Tang et al. 2008; Yamagishi/Yamagishi 1994). Reputational losses would be fatal for certification authorities due to the high degree of competition in the certification market (Zhao et al. 2009). When source reputation is high, the information presented by the source is perceived to be useful (Ko et al. 2005). Customers integrate the available information from reputable certification authorities with information about the CSP to generate their overall perceptions (Anderson 1981). Customers use the source of the assurance seals to apply weights and prefer those issued by highly reputable third parties (Kimery/McCord 2002a; Lala et al. 2002; Lowry et al. 2008). Customers also associate positive perception regarding the third-party with the lesser-known or even unknown CSPs (Lowry et al. 2008; Simonin/Ruth 1998). A certification authority's high reputation increases the perceived effect of the communicated audit for the protection of customers' privacy and positively influences the perceived privacy in a professional cloud environment:

> ***Hypothesis 1 (H1):*** *Customers' perceived privacy of cloud service providers is a positive function of the certification authorities' reputation as the quality level of an audit remains constant.*

9.2.2.4 Quality level of an assurance seal audit

The certification authorities provide assertions through audits about the ability and the state of the CSP to secure and protect data (Oezpolat et al. 2013). While some assurance seals are based on a high quality level of an audit including an in depth certification process, e.g. the ISO 27001, TRUSTe, WEBTRUST or CyberTrust seal, others are based on a low quality level of an audit that only publishes a directory of trusted online retailers, e.g. BBB On-Line (Oezpolat et al. 2013). With more effort made in verifying the security of the CSP, the certification authorities improve their security and privacy knowledge and technologies (Anderson/Moore 2006). With the increasing quality level of an audit, the ability to observe a privacy breach increases (Lee et al. 2013a). Based on this information, customers understand why assurance seals in place are valid and reliable in effectively protecting their privacy (Kim/Benbasat 2006). When the quality level of an audit is high, customers value the information more in comparison to if the quality level of an audit is low (Kim/Benbasat 2006). This holds particularly true in an ever-changing cloud environment where customers doubt the validity and reliability of audits with a low quality level (Lins et al. 2016; Anisetti et al. 2017). Similar to our previous argumentation, customers integrate the information about the quality level of an audit conducted by a certification authority with the information about privacy protection activities of the CSP to generate their overall perceptions (Anderson 1981). A high quality level of an audit signals successful protection of customers' privacy and, therefore, positively influences the perceived privacy in a professional cloud environment:

> ***Hypothesis 2 (H2):*** *Customers' perceived privacy of cloud service providers is a positive function of the quality level of an audit as the certification authorities' reputation remains constant.*

9.2.3 Effective form of assurance seals

Customers integrate information about the reputation of a certification authority and its quality level of an audit to form their overall perception. Customers value information like the quality level of an audit to understand why an item of information is valid and reliable (Kim/Benbasat 2006). Moreover, depending on the source of information, information differs in terms of the relevance to the customer (Lowry et al. 2008). The certification authority's reputation does not itself produce a change of opinion, but affects the degree of the stimulus resulting from the quality level of an audit (Anderson 1971). Similar to our previous argumentation, customers integrate these pieces of information with the information about the cloud service to generate their overall perceptions (Anderson 1981). A highly reputable certification authority that conducts a high quality level of an audit outperforms a low (highly) reputable certification authority that conducts a high (low) quality level of an audit in terms of perceived privacy in a professional cloud environment:

> ***Hypothesis 3 (H3):*** *Customers' perceived privacy of cloud service providers is higher for highly reputable certification authorities that conduct a high quality level of an audit than for a low (highly) reputable certification authority that conducts a high (low) quality level of an audit.*

Our research model is illustrated in Figure 16.

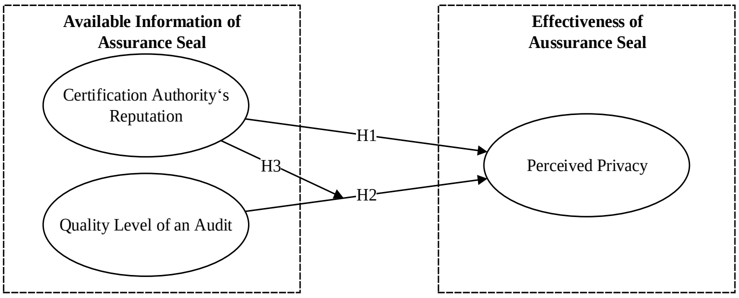

Available Information of Assurance Seal
Certification Authority's Reputation
Quality Level of an Audit
H1
H2
H3
Effectiveness of Aussurance Seal
Perceived Privacy

Figure 16. Proposed research model to investigate the effectiveness of assurance seals

9.3 Research method

9.3.1 Research design

We used an experimental design because it allows for the manipulation of variables and the testing of causal relationships. We used a within-subject experimental design to control for subject variability (it accounts for individual differences when subjects serve as their own control) (Keppel 1991). In addition, a within-subject design provides us the opportunity to simulate repeated decisions, a frequently occurrence in real life (Andriole 2007). Specifically, we employed a 2 (high/ low certification authorities' reputation) X 2 (high/ low quality level of an audit) within-subject factorial design. We also employed a baseline scenario without any manipulation (see Figure 17).

9.3.2 Experiment manipulations

The reputation of certification authorities and the quality level of an audit were operationalized using an online-based free simulation experiment combined with the scenario-based method. Whereas standard laboratory experiments rely on a treatment to vary one or more independent variables, free simulation experiments expose the subjects to a number of realistic tasks – for example, by identifying an appropriate CSP. A core feature of free simulation experiments is the interaction of subjects with a simulated website; this feature is frequently used in online studies to increase realism and generalizability (Gefen et al. 2003; Burton-Jones/Straub 2006; Lowry et al. 2012). Website conditions ranged freely and widely as subjects interacted naturally although all subjects received treatment materials. The realistic task and the natural interaction allow subjects to form meaningful perceptions before answering related questions (Gefen et al. 2003; Söllner et al. 2015).

Scenarios illustrate possible states of a cloud service. Scenarios provide a form or tool to study a possible and plausible state, and to create awareness of which applications are possible (Bria et al. 2001). Free-simulated online experiments, including different scenarios, are frequently used in experimental studies to manipulate different conditions of variables, simulate customers tasks or represent context for study (Lowry et al. 2012; Xu et al. 2012b). We used five scenarios in a free-simulated online experiment to investigate which information determine the effectiveness of assurance seals to protect privacy.

		Certification authorities' reputation	
		low	high
Quality level of an audit	low	(1)	(2)
	high	(3)	(4)

A baseline scenario with no manipulation was also simulated (5)

Figure 17. Research design

We manipulated the certification authorities' reputation and the quality level of an audit using four variant scenarios. We added a baseline scenario in which no manipulation occurred. To vary certification authorities' reputation, we used certification authorities with high (e.g., TÜV – international well-known certification authority) versus low (e.g., CERTIFYER[3] – newly developed certification authority[4]) reputation.

To vary the quality level of an audit, we used different attestation processes and related attestation timings: an attestation through a static certification (e.g., attestation took place 2

[3] The name of the newly developed certification service was blinded for confidential reasons.

[4] Lowry et al. (2008) provide empirical evidence that the reputation of unknown third-parties is significantly lower than the reputation of a known and highly reputable organization.

years ago) and a continuous certification which was continuously updated (e.g., attestation took place 1 week ago). Since continuous certification involves "high efforts for agent development and implementation" (Lins et al. 2016) for the audit and high effort for the continuous verification and attestation process, the quality level of an audit for a continuous certification is higher than for the a static certification.

Overall, a total of four manipulated scenarios and one baseline scenario were presented to subjects: (1) low certification authorities' reputation and low quality level of an audit; (2) high certification authorities' reputation and low quality level of an audit; (3) low certification authorities' reputation and high quality level of an audit; (4) high certification authorities' reputation and high quality level of an audit. To assure comparable results, we used ISO 27001 as a well-known certification scope for all four scenarios. The last scenario was a baseline scenario in which no manipulation occurred (5).

Two variables, certification authorities' reputation and quality level of an audit, were manipulated in the experiment. The manipulation was illustrated within two different levels of detail. First, each manipulation was on the scenarios' main page as an assurance seal, identification of certification authority, certification scope and identification of attestation process. Second, each manipulation was accessible within the certification attestation report. As an example, Figure 18 illustrates scenario (3) including the possible navigations to the certification attestation report.

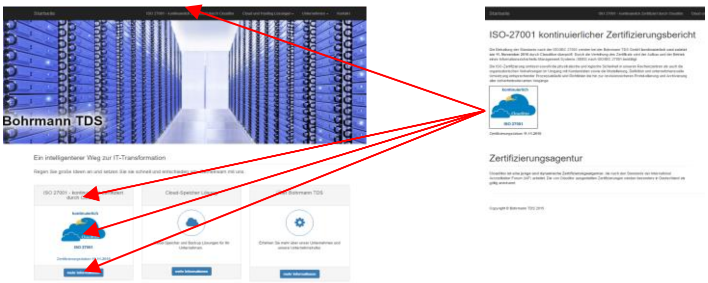

Bohrmann TDS
Ein intelligenterer Weg zur IT-Transformation
Cloud-Speicher Lösungen
ISO 27001
ISO-27001 kontinuierlicher Zertifizierungsbericht
Zertifizierungsagentur

Figure 18. The main page of scenario (3) (left) including possible navigation paths (red arrows) to certification attestation report (right)

Each certification attestation report consists of three major parts. First, the certification process was described including the last attestation date. Second, background information (size and acting regions) on the certification authority was provided. Third, some background information about the ISO 27001 certification was provided; this information was not changed across all manipulations, ensuring a common understanding regarding the assurance seal and attestation report that is in place (Lowry et al. 2012).

9.3.3 Measurement

The measurement of formative constructs is highly dependent on the related domain (Petter et al. 2007). To provide comparable results for privacy across different domains, we used a reflective construct (Siponen/Vance 2014). For our dependent variable, we used the three reflective measurements of perceived privacy from Dinev et al. (2013) and adapted the wording to a professional cloud environment (see Table 37).

Constructs and items (measured on a seven-point, Likert-type scale)		**Source**
Perceived privacy	I feel I have enough data privacy when I use this cloud service provider.	Dinev et al. (2013)
	I am comfortable with the amount of data privacy with this cloud service provider.	
	I think data privacy is preserved when I use this cloud service provider.	
Manipulation check – reputation	In this scenario, the certification authority has a high reputation in the market.	Self-developed
Manipulation check – quality level of an audit	In this scenario, the certification process was based on a continuous certification process. (measured on a yes/no scale)	Self-developed

Table 37. Measurement items and manipulation checks

Since not all subjects were fluent in English, the experiment as well as the questionnaire were provided in German. To check for translation bias within the measurement items, a back-translation technique was employed in which two different translators translated the German questionnaire back into English (Bhattacherjee/Park 2014). The back-translated items had a high degree of correspondence with the original English items (see Table 37) assuring the relative lack of translation bias.

9.3.4 Research procedures

Approximately two months before initiating the experiment each subject received an e-mail with a personalized pre-experiment survey link inviting them to sign up for the experiment. During this phase, we received their consent to participate, and we collected the pre-experiment measures to reduce the risk of common methods bias (Podsakoff et al. 2003). The pre-experimental measures included cloud computing experience, and familiarity with ISO 27001 certification. The latter was important to assure each subject understood the meaning and sense of the ISO 27001 assurance seal (Lowry et al. 2012). Because we collected this information prior to the experiment, the experimental site did not influence these measures. Figure 19 illustrates the entire research process.

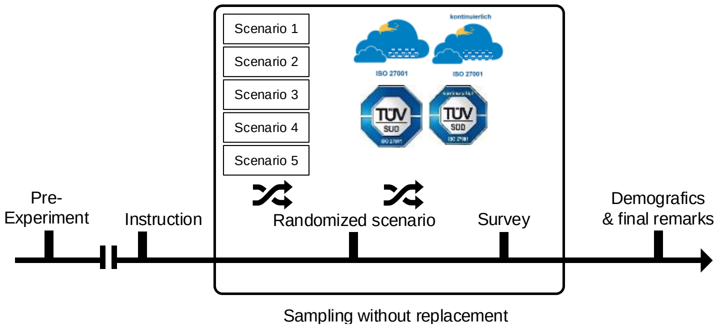


Figure 19. Research procedures

During the experiment, all subjects received and read the same instructions. Subjects were asked to identify an appropriate CSP that offers cloud storage for their data. Subsequently, each subject was presented with five scenarios of CSP websites in which – except for the baseline condition – different certification authorities' reputation (high versus low) were offered with different quality levels of an audit (high versus low). The presentation of each scenario was followed by a survey. This included manipulation check questions and questions that measured the subject's perceived privacy based on the presented scenario (see Table 37). Each subject was asked to answer the questionnaire in regard to the experienced scenario. The last part of the experiment captured subjects' demographic information (e.g., age and gender) and final remarks.

To minimize possible learning and ordering effects of scenarios on subjects, we considered three strategies. First, we presented the scenarios in a randomized order. Second, subjects were asked, after each scenario and at the end of the experiment, an open question asking which information they used as a basis for their judgments and if any irregularities occurred. Last, we tracked each subject's duration time to navigate through our experimental websites. The average duration time of subjects within each scenario was 3.8 minutes; subjects navigated through our experimental websites, including the attestation report, without any obvious patterns. No evidence of learning or ordering effects were observed.

We carried out a pilot study with research fellows to evaluate the clarity of the scenarios and the items in the questionnaire. No major issues were identified during the pilot study; the pilot subjects made minor suggestions on wording and phrasing that were incorporated into the questionnaire and experimental websites. After another review round, we conducted the experiment.

9.3.5 Subjects

We adopted a purposive sampling technique. This is a non-probability sampling that conforms to certain criteria (Cooper/Emory 1995). Previous studies have suggested that certificates are only effective when subjects understand their meaning and sense (Lowry et al. 2012). To confirm these preconditions, we focused on professional cloud decision makers. Therefore, our reason for choosing purposive sampling is that professional cloud decision makers are rare and only selected subjects are suitable for our study.

Subjects were recruited from medium- and large-sized German companies across different industries. 71 suitable subjects were identified and contacted. Finally, a total number of 43 subjects participated in this study. All subjects were native German speakers. Demographic information and the cloud experience of the subjects is presented in Table 38.

The subjects recruited in this study had extensive cloud experience and were familiar with the certificate ISO 27001 (see Table 38). All subjects' job descriptions were related to selecting and purchasing cloud-services. This ensures reliable results based on experienced professionals within a cloud environment (Siponen/Vance 2014).

Demographics		**Frequency**	**Percent**	**Experience**		**Frequency**	**Percent**
Age	<31	6	14	Professional cloud experience	<2 years	10	23
	31-40	9	22		3-5 years	15	35
	41-50	14	32		6-8 years	11	25
	>50	14	32		>8 years	3	7
Sex	Female	3	7	Certificate familiarity	yes	43	100
	Male	40	93		no	0	0

Table 38. Demographic and experience information of subjects

Assuming a medium effect size ($f = 0.25$), with a power of 0.80 at alpha equals 0.05 significance level, the required sample size for each cell is 39 (Cohen 1992). Hence, 43 subjects for each experimental treatment is adequate for data analysis.

9.3.6 Manipulation checks

The manipulation of certification authorities' reputation and the quality level of an audit was assessed following the presentation of each scenario (see Table 37 for the manipulation check questions). These questions were used to test the subjects' interpretation and understanding of the scenarios.

We conducted paired-sample T-tests to test the effectiveness of the manipulations. The results show that all treatments were manipulated effectively. First, subjects perceived scenarios in which TÜV served as a certification authority to have a higher reputation than those scenarios with the low certification authorities' reputation CERTIFYER (mean difference = 2.69, std. deviation = 0.44, $t = 6.05$, $p < 0.05$). Second, subjects perceived that those scenarios with a continuous certification provided greater perception regarding the continuous and up-to-date attestation of third-party certification than the static certification scenarios (mean difference = 0.79, std. deviation = 0.24, $t = 3.22$, $p < 0.05$).

9.3.7 Factor analysis

The reflective construct perceived privacy is validated using the standard procedure documented by Straub (1989). All factor loadings are significant suggesting convergent validity. Perceived privacy satisfies the threshold values for the average variance extracted (AVE > 0.50) and Cronbach's alpha (alpha > 0.70) as suggested by Straub (1989). To evaluate construct reliability, we calculated composite reliability (CR) for perceived privacy. Perceived privacy has a composite reliability significantly above the cut-off value of 0.70. In sum, perceived privacy's quality is satisfactory.

9.4 Results

9.4.1 Testing the research model

Data associated with perceived privacy was analyzed using a repeated-measure ANOVA test with two within-subject factors as independent variables: certification authorities' reputation and the quality level of an audit. The mean values and standard deviations are reported in Table 39.

Within-subject factors		**Perceived privacy**	
Certification authorities' reputation	**Quality level of an audit**	**Mean**	**Standard deviation**
Baseline (no treatment)	Baseline (no treatment)	3.124	0.229
Low reputable certification authority	Static certification	3.419	0.254
	Continuous certification	4.101	0.267
High reputable certification authority	Static certification	3.829	0.218
	Continuous certification	4.512	0.255

Table 39. Means and standard deviations for perceived privacy

To test Hypotheses 1, a contrast test was conducted based on the Wilks-Lambda test (Kirk 1982). H1: *Customers' perceived privacy of cloud service providers is a positive function of the certification authorities' reputation as the quality level of an audit remains constant*, is supported. Table 40 reports for the manipulation contrast test for perceived privacy a contrast value = 0.746, F-Value = 14.274 and p-Value < 0.001.

To test Hypotheses 2, a contrast test was conducted based on the Wilks-Lambda test (Kirk 1982). H2: *Customers' perceived privacy of cloud service providers is a positive function of the quality level of an audit as the certification authorities' reputation remains constant*, is also supported. Table 40 reports for the manipulation contrast test for perceived privacy a contrast value = 0.908, F-Value = 4.236 and p-Value < 0.05.

Hypothesis	**Contrast value**	**F-Value**	**p-Value**	**Hypothesis supported?**
H1	0.746	14.274	<0.001	Yes
H2	0.908	4.236	0.023	Yes

Table 40. Manipulation contrast tests for perceived privacy

To test Hypotheses 3, two further contrast tests were conducted based on the Wilks-Lambda test (Kirk 1982). H3: *Customers' perceived privacy of cloud service providers is higher for highly reputable certification authorities that conduct a high quality level of an audit than for a low (highly) reputable certification authority that conducts a high (low) quality level of an audit*, is supported. In this analysis, we first (a) compared certification authorities of high reputation and high quality level of an audit with certification authorities of high reputation and low quality level of an audit. Table 41 reports for the manipulation contrast test for perceived privacy a contrast value = 0.804, F-Value = 10.223 and p-Value < 0.05. We second (b) compared certification authorities of high reputation and high quality level of an audit with certification authorities of low reputation and high quality level of an audit. Table 41 reports for the manipulation contrast test for perceived privacy a contrast value = 0.927, F-Value = 3.299 and p-Value < 0.1.

Hypothesis	Contrast test between certification authorities	Contrast value	F-Value	p-Value	Hypothesis supported?
H3	(a) high reputation and low quality level of an audit against high reputation and high quality level of an audit	0.804	10.223	0.001	Yes
	(b) low reputation and high quality level of an audit against high reputation and high quality level of an audit	0.927	3.299	0.038	

Table 41. Additional manipulation contrast tests for perceived privacy

9.4.2 Additional analysis

To test if any assurance seal influences customers' perceived privacy, four baseline contrast tests were conducted based on the Wilks-Lambda test (Kirk 1982). Certification authorities of high reputation and low quality level of an audit (contrast value = 0.615, F-Value = 26.248, p-Value < 0.001), low reputation and high quality level of an audit (contrast value = 0.750, F-Value = 14.032, p-Value < 0.001) and high reputation and high quality level of an audit (contrast value = 0.421, F-Value = 55.503, p-Value < 0.001), perceived privacy was significantly higher than of the perceive privacy rating of the baseline scenario. Perceived privacy resulting from low certification authorities' reputation and low quality level of an audit was higher on a marginally significant level (contrast value = 0.926, F-Value = 3.371, p-Value < 0.05) than the baseline scenario as well (see Table 42). Therefore, within our experiment any assurance seal can increase customers' perceived privacy in a professional cloud environment.

Baseline contrast test against certification authorities of:	Contrast value	F-Value	p-Value
… low reputation and low quality level of an audit	0.926	3.371	0.036
… high reputation and low quality level of an audit	0.615	26.248	<0.001
… low reputation and high quality level of an audit	0.750	14.032	<0.001
… high reputation and high quality level of an audit	0.431	55.503	<0.001

Table 42. Baseline contrast tests for perceived privacy

9.5 Discussion

9.5.1 Findings

Our research demonstrates that a customers' perceived privacy in a professional cloud environment can be increased by the provisioning of relevant information through assurance seals provided by an independent certification authority. Therefore, the customers' perceptions and beliefs regarding the assurance seal are not replaced by new information of the unknown CSP, rather old perceptions and beliefs of the source, and semantic properties of an assurance seal are integrated with the information to form new attitudes regarding the unknown CSP.

Our findings suggest that certification authorities' reputation and the quality level of an audit are important information to shape customers' perceptions, including perceived privacy and, in doing so, determine the effectiveness of assurance seals in a professional cloud environment. When the certification authorities' reputation and the quality level of an audit are high, the highest effects of assurance seals on customers' perceived privacy are identified during CSP selection.

9.5.2 Study contribution and theoretical and managerial implications

Our findings extend research by explaining how semantic properties of assurance seals are integrated to form customers' perceptions. Customers are not only able to differentiate between high and low levels of source reputation, also about high and low levels of semantic properties of assurance seals. In particular, information in regard to the reliability and validity of an assurance seal are important semantic properties that contributes to the attitudinal judgment. Consistent with the information integration theory (Anderson 1981), third-parties' reputation does not alone produce opinion change and determine assurance seals effectiveness (Lowry et al. 2008), it rather influences the effect size of the opinion change on how and what interaction the third-party has.

Our findings extend research by considering semantic properties of assurance seals. To protect privacy in a professional cloud environment, customers not only consider "who" provides which assurance seal, they also consider "how" the assurance seal is reached. Hence, as customers face information asymmetry and cannot assure privacy by themselves, semantic properties are important to evaluate the validity and reliability of an assurance seal. Therefore, when investigating the effectiveness of assurance seals in online environments the information who protect what and how should be considered and communicated.

However, we notice that perceived privacy resulting from low certification authorities' reputation and low quality level of an audit was higher on a marginally significant level than the baseline scenario having no assurance seal. Such findings are in line with the inconsistent findings in literature (Oezpolat et al. 2013). Therefore, we conclude, research should be careful in selecting assurance seals of low reputable certification authorities or low quality level of an audit when investigating assurance seals.

From a practitioner point of view, our results suggest that CSPs can influence perceptions of their customers by implementing assurance seals. Hence, CSPs should consider certification authorities to prove their data protection capabilities. However, not all assurance seals influence the perception of customers in the same manner. CSPs should particular choose assurance seals with a high quality level of an audit like continuous certificates issued from a high reputable certification authority.

Our results also provide conclusion for certification authorities. To be effective, any certification authority need to use a certain strategy to communicate their reputation and quality level of an audit. Our study shows that the usage of certificates combined with an attestation report is one effective example for such a communication strategy. An assurance seal including the certification scope, certification method and certification authority in combination with a certification attestation report is effective in creating a retrieval cue for customers' privacy perception.

9.5.3 Limitations and future research

All research is subject to limitations. Here, one possible limitation of our work relates to the method used to operationalize high and low certification authorities' reputation and quality level of an audit. We used scenarios to manipulate the different conditions of high and low certification authorities' reputation and quality level of an audit. Scenarios were presented to the subjects before capturing their perceived privacy. One may argue that a real CSP website will provide a more realistic experience to subjects and produces more reliable and meaningful results. However, considering that continuous certification to provide high quality level of an audit is still very new and not readily available, the scenario-based approach allows us to study this emerging phenomenon without the constraints of time and state-of-the-art technology.

This study was conducted in Germany. Therefore, care must be taken when attempting to generalize the privacy results to other social, economic, legal and cultural environments. Privacy is a relative concept and may be related to cultural values (Kim et al. 2015) – what is considered private in one culture or legal region may not be considered private in another culture or legal region. For example, people in the United States tend to take the perspectives of "privacy pragmatists" while Europeans (including Germans) are concerned about their privacy and are more likely to take the perspectives of "privacy fundamentalists" (Galanxhi/Nah 2006).

Last, our limited number of subjects were recruited using a purposive selection approach. While our professionals were all familiar with assurance seals, future research can take this investigation further by drawing research subjects from a more diverse, randomly selected, and comprehensive population.

9.6 Conclusion

This research investigates the influence of assurance seals on customers' perceived privacy within a professional cloud environment. By focusing on the two information dimensions certification authorities' reputation and the quality level of an audit, this research has important theoretical and managerial implications. Results of this study are important in situations when customers face information asymmetry and cannot assure privacy by themselves.

From a theoretical point of view, our research extends the information integration theory by demonstrating how source reputation affects customers' perceived privacy resulting from information how a third-party and an unknown CSP interact. Second, we provide an empirical evidence about the effectiveness of assurance seals within a professional cloud environment. Third, this research provides two information dimensions, namely certification authorities' reputation and the quality level of an audit, which interact and determine the effectiveness of assurance seals in a cloud environment. From a managerial point of view, we contribute to CSPs and certification authorities.

Acknowledgement

This research was funded by the German Federal Ministry for Education and Research (grant. No. 16KIS0078).

Part C

10 Summary of Results

Based on our argumentation that a poor understanding about the decision-making during CSP selection is a major cause for the low and different adoption rate of cloud services in different cultures, this thesis addresses several research gaps in the field of ITO in general, and specifically of cloud sourcing. We obtained the following research results:

(1) **Identification of Control Mechanisms in an Online Environment:** P1 was motivated by a fragmented body of knowledge, in which recent investigations largely examined perceptions independently from the mechanisms and the concept itself. Based on this fragmented research, a conceptual consensus for control mechanisms is missing, even if control mechanisms are an important element of relational governance. To address these gaps, P1 consists of a systematic literature review, and identified examples of control mechanisms, as reported in IS literature.

Based on this comprehensive overview, P1 provides insights of the interrelation of existing assurance research and offer insights into how control mechanisms can be conceptualized. Further, P1 provides a theoretical framework to consider the concepts of control mechanisms and how these concepts are related to the antecedents and effects of control mechanisms.

(2) **Comparing Selection Criteria in ITO and CC:** The conduction of P2 was motivated by a poor understanding of the validity of existing ITO provider selection criteria within the context of CC. In order to enhance understanding of this issue, P2 used a Delphi study approach to identify criteria of importance to experts when selecting CSP.

P2 yielded the identification and ranking by importance of 13 CSP selection criteria. We further show that our results for CSP selection criteria represent ITO provider selection criteria for a technology-enabled and market-based outsourcing arrangement. Therefore, P2 supports prior findings that CC can be seen as an evolution and specific form of ITO and the rich body of ITO knowledge should be leveraged within the context of CC.

(3) **CSP Selection Criteria:** Using an exploratory Delphi study design, P3 investigated the most important QoS attributes for the selection of CSP as identified by a panel of professionals. Through consensus, in P3 we identified the 13 most important QoS attributes for CSP selection and ranked their importance in 2015. P3 showed that results for QoS attributes comprise technical QoS attributes and managerial QoS attributes, both of which are important during CSP selection.

P3 shows that cloud customers require an extensive variety of managerial QoS attributes during CSP selection. This finding supports prior research on cloud customer uncertainty in an ever-changing cloud environment. Further, a comparison of the most important QoS attributes in this study with those reported in previous studies identifies the following four key changes that take place within the cloud market: (1) The importance of increasing data protection; (2) The cloud customer’s pursuit of value co-creation CSP; (3) The possibility of a decrease in CSPs' opportunistic behavior; and (4) Product uncertainty remains a major problem during CSP selection.

(4) **Control Agents Influence on Decision Makers' Perceived Privacy:** Results of P4 provide insights into effective control agents operating within a cloud environment. P4 differentiates between three control agents (personal control, proxy control, and collective control), and investigates their influences on cloud customers' perceived control over sensitive information and privacy during cloud sourcing.

Although proxy and collective control influence cloud customers, P4 identified no support from the customers used in our sample for personal control. Hence, only external control agents, which are known to be able to apply sanctions, are perceived to be effective. Furthermore, P4 identified the mediation effects of perceived information control between control agents and privacy.

(5) **Cultural Difference Influence Decision Makers Choice of Control Mechanisms:** P5 demonstrates that cloud customers in high uncertainty avoidance cultures prefer institutional control and the power of the marketplace to increase their perceived information control and perceived privacy. By contrast, cloud customers in low uncertainty avoidance cultures prefer direct control and institutional control to increase their perceived information control and perceived privacy. P5 shows that the power of the marketplace has a significant higher effect in high uncertainty avoidance cultures compared to low uncertainty avoidance cultures. Direct control has a significantly higher effect in low uncertainty avoidance cultures compared to high uncertainty avoidance cultures.

(6) **Effects of Cloud Assurance Seals on Customers' Perceived Privacy:** P6 investigates the influence of assurance seals on customers' perceived privacy within a professional cloud environment. By focusing on the two information dimensions certification authorities' reputation and the quality level of an audit, this research has important theoretical and managerial implications. Results of P6 are important in situations when customers face information asymmetry and cannot assure privacy by themselves.

P6 demonstrates that a customers' perceived privacy in a professional cloud environment can be increased by the provisioning of relevant information through assurance seals provided by an independent certification authority. Therefore, the customers' perceptions and beliefs regarding the assurance seal are not replaced by new information of the unknown CSP, rather old perceptions and beliefs of the source, and semantic properties of an assurance seal are integrated with the information to form new attitudes regarding the unknown CSP. P6 suggests that certification authorities' reputation and the quality level of an audit are important information to shape customers' perceptions, including perceived privacy and, in doing so, determine the effectiveness of assurance seals in a professional cloud environment. When the certification authorities' reputation and the quality level of an audit are high, the highest effects of assurance seals on customers' perceived privacy are identified during CSP selection.

Table 43 gives an overview on the key findings of this thesis.

Publication	Findings
P1	• Characterization of control mechanisms in an online environment o Identification of 15 control mechanisms o Categorization of control mechanisms into personal control, proxy control, and collective control o Identification of antecedents and effects of control mechanisms in an online environment
P2	• Identification of similarities and differences between ITO and cloud sourcing o Identification of 13 CSP selection criteria o CSP selection criteria represent ITO provider selection criteria for a technology-enabled and market-based outsourcing arrangement
P3	• Empirical ranking of QoS attributes from customers perspective o QoS attributes comprise technical QoS attributes and managerial QoS attributes, both of which are important during CSP selection o CSP selection framework based on technical and managerial QoS attributes • Four key changes that take place within the cloud market o The importance of increasing data protection o The cloud customer's pursuit of value co-creation CSP o The possibility of a decrease in CSPs' opportunistic behavior o Product uncertainty remains a major problem during CSP selection
P4	• Differences between three control agents o Personal control o Proxy control o Collective control • Only external control agents, which are known to be able to apply sanctions, are perceived to be effective importance of increasing data protection o Proxy and collective control influence cloud customers o No support from the customers used in our sample for the effectiveness of personal control • Mediation effects of perceived information control between control agents and privacy
P5	• Investigates the cross-cultural formation of perceived privacy from decision makers during the selection of CSPs in cloud sourcing projects o Decision makers from low uncertainty avoidance cultures rely more on their own competence to form privacy perceptions o Decision makers from high uncertainty avoidance cultures tend to rely more on the power of the marketplace to form their privacy perceptions

	o Institutional controls affect decision makers’ perceived privacy across all cultures
P6	• Customers’ perceptions and beliefs regarding the assurance seal are not replaced by new information of the unknown CSP, rather old perceptions and beliefs of the source, and semantic properties of an assurance seal are integrated with the information to form new attitudes regarding the unknown CSP • Determine the effectiveness of assurance seals in a professional cloud environment o Certification authorities’ reputation and the quality level of an audit are important information to shape customers’ privacy perceptions, determine the effectiveness of assurance seals in a professional cloud environment o When the certification authorities’ reputation and the quality level of an audit are high, the highest effects of assurance seals on customers’ perceived privacy are identified during CSP selection

Table 43. Overview on Key Results

11 Study Limitations

This thesis is subject to limitations. A detailed discussion of these limitations is provided at the end of each publication in part B of this thesis. In the following, we summarize the major limitations along the four major attributes that characterize the validity of a research study in general (Bhattacherjee 2012): internal validity, external validity, construct validity, and statistical conclusion validity. In this section, each of these validity types is briefly described and it is discussed how threats to these validities could potentially affect the findings of this thesis and the implications from these findings. It is further evaluated how these threats to validity should be addressed in future research. Table 44 summarizes the potential validity threats to the findings of this thesis.

Internal validity. Internal validity examines to what degree the observed change in a dependent variable is caused by a change in the independent variable and not by changes in the environment or other factors (Bhattacherjee 2012). There are three conditions for internal validity (Bhattacherjee 2012). First, covariation (e.g., correlation, in linear relationships) between cause (independent variable) and effect (dependent variable). Second, cause precedes effect in time. Third, all other explanations are ruled out. Internal validity is a general problem of all non-experimental empirical research (Gravetter/Forzano 2003). Whereas it is generally feasible to satisfy the first two conditions (covariation and temporal precedence) by non-experimental studies, all rival explanations can only be reliably ruled out in controlled experimental settings (Gravetter/Forzano 2003).

Consequently, publications P1-P5 are potentially affected by internal validity threats and should be interpreted accordingly. The data analysis in P1 might be subjective biased and care must be taken by interpreting the relationships and classifications. Furthermore, not all studies that were included in this review used experimental methods to reduce internal validity threats. P2 and P3 are subject to limitations regarding their internal validity since only a moderate consensus have been reached. P4 and P5 was conducted in an uncontrolled environment that threat its internal validity.

External validity. External validity examines to what degree the observed associations can be generalized from the sample to the population (population validity) and to other people, organizations, contexts and time (ecological validity) (Bhattacherjee 2012).

P1 was limited to a number of outlets and databases that limits the generalizability of these results. P2 and P3 used a purposive sampling technique considering different industries, service models, and company sizes that limits also the generalizability of those results. P4 was conducted in Germany and is therefore limited to decision makers having a certain cultural background.

Concerning ecological validity, P2-P6 are conducted in a professional cloud environment. Hence, generalizing the results to other populations, such as end-customers, may require additional research.

Construct validity. Construct validity examines to what degree a measure is actually representing the intended construct and not another construct (Bhattacherjee 2012).

P1 summarizes the findings of empirical research. Even if all included studies provide certain evidences (e.g., Cronbach's alpha) to assure construct validity, inappropriate conclusions are possible. P4-P6 used constructs to measure decision makers' perceived privacy and further independent variables. Even if this thesis used constructs adopted from literature, the actual measurement and the intended measurement could be different.

Statistical conclusion validity. Statistical conclusion validity examines the extent to which conclusions derived using a statistical procedure is valid (Bhattacherjee 2012).

Both, P4-P6 may face the threat of Type I or Type II error. Type I error is when we conclude that there is a relationship between two variables and we reject a true null hypothesis when in reality, there is no relationship between the two variables. If we fail to reject a false null hypothesis that is actually true it is called Type II error. Hence, care must be taken when interpreting the relationships. Both errors could have occurred during the data analysis of P4-P6.

Publication	**Internal validity**	**External validity**	**Construct validity**	**Statistical conclusion validity**
P1	• Not exclusively experimental data • Subjective biased analysis	• Limited number of outlets and database	• Measurement error	• Type I error • Type II error
P2	• Non-experimental data • Moderate consensus among panelists	• Purposive sampling technique • Professional environment		
P3	• Non-experimental data • Moderate consensus among panelists	• Purposive sampling technique • Professional environment		
P4	• Non-experimental data • Uncontrolled environment	• German sample • Professional environment	• Measurement error	• Type I error • Type II error
P5	• Non-experimental data • Uncontrolled environment	• Western sample • Professional environment	• Measurement error	• Type I error • Type II error
P6		• Professional environment	• Measurement error	• Type I error • Type II error

Table 44. Summary of potential validity threats

12 Contributions of this Thesis

12.1 Contributions to Theory

A detailed discussion of this thesis contribution to theory is provided at the end of each publication in part B of this thesis. In the following, we summarize the major theoretical contributions along the four major building blocks of theory development (Whetten 1989): (1) variables that should be included in explaining a phenomenon of interest, (2) relationships between these variables, (3) reasoning behind these relationships, and finally, (4) subject-related, geographical, and temporal boundaries under which a theory is valid. This section summarizes the theoretical contribution of this thesis and its embedded publications alongside these building blocks.

> **Variables:** P1 identify and conceptualize control mechanisms (personal control, proxy control, and collective control), their antecedents (concerns) and effects (beliefs, intentions, behavior). Such integrated view provides a coherent and cumulative body of work of studies within an online environment and, therefore, extends prior work on control mechanisms (Noordewier et al. 1990; Dyer 1997; Gundlach/Cannon 2010).
>
> P2 and P3 point out important mechanisms within a cloud environment. P2 and P3 identified the most important selection criteria used from a decision makers perspective during CSP selection decisions. Since CC is a technology-enabled and market-based outsourcing arrangement via the internet, P2 identified that decision makers need a greater amount of control mechanisms, in comparison to ITO decision makers, as the importance of capacity of operations increases for conceptually related CSP selection criteria (Chang et al. 2012; Gopal/Koka 2012). Moreover, a comparison of the most important QoS attributes in P3 with those reported in previous studies (Repschlaeger et al. 2013; Saripalli/Pingali 2011) identifies the following four key changes that take place within the cloud market: (1) The importance of increasing data protection; (2) The cloud customer's pursuit of value co-creation CSP; (3) The possibility of a decrease in CSPs' opportunistic behavior; and (4) Product uncertainty remains a major problem during CSP selection.
>
> P4 and P5 extend literature on privacy by identifying perceived information control as a mediator between control agents and privacy within a professional cloud environment in different cultures. Research on privacy has previously been conducted mainly within a consumer context (Dinev et al. 2013), although professionals also struggle with privacy issues (Goodman 2000). Our findings provide evidence of the importance of privacy within a professional context and demonstrate the importance of considering the mediating effects of control perception when investigating privacy protection through different control agents and the privacy protection mechanisms used. Moreover, results from P4 and P5 extend literature on control by considering different control agents. As indicated by Gregory/Keil (2014), we argue that although different control agents are important, the differences between their effectiveness should be considered.

Relationships: P1 provides a theoretical framework to consider the concepts of control mechanisms and how these concepts are related to the antecedents and effects of control mechanisms. Therefore, P1 posits that three sets of control mechanisms – personal control, proxy control, and collective control – influence individuals' beliefs, intentions, and behaviors when concerns are in place.

P4 and P5 analyze cloud sourcing decision-making by investigating how individuals' perception of control and privacy influences their purchasing decisions. P4 demonstrates how cloud customers control sensitive information and ensure privacy within a cloud environment. P5 extends such findings by demonstrating the influence of different control mechanisms on cloud customers' privacy perceptions within different cultures. Such findings are vital for cloud research because they show how different actors in different cultures influence the cloud sourcing decisions made by cloud customers.

Findings of P6 extend research by explaining how semantic properties of assurance seals are integrated to form customers' perceptions. Customers are not only able to differentiate between high and low levels of source reputation, also about high and low levels of semantic properties of assurance seals. In particular, information in regard to the reliability and validity of an assurance seal are important semantic properties that contributes to the attitudinal judgment. Consistent with the information integration theory (Anderson 1981), third-parties' reputation does not alone produce opinion change and determine assurance seals effectiveness (Lowry et al. 2008), it rather influences the effect size of the opinion change on how and what interaction the third-party has. However, P6 notices that perceived privacy resulting from low certification authorities' reputation and low quality level of an audit was higher on a marginally significant level than the baseline scenario having no assurance seal. Such findings are in line with the inconsistent findings in literature (Oezpolat et al. 2013). Therefore, P6 concludes, research should be careful in selecting assurance seals of low reputable certification authorities or low quality level of an audit when investigating assurance seals.

Reasoning: P5 explains why differences on the effectiveness of control mechanisms to form customers' perceptions in different countries occur. Customers from low uncertainty avoidance cultures rely more on their own competence to form privacy perceptions. By contrast, customers from high uncertainty avoidance cultures tend to rely more on the collective to form their privacy perceptions. Surprisingly, proxy control affect decision makers' perceived privacy across all cultures. P6 extends research by considering semantic properties of assurance seals. To protect privacy in a professional cloud environment, customers not only consider "who" provides which assurance seal, they also consider "how" the assurance seal is reached. Hence, as customers face information asymmetry and cannot assure privacy by themselves, semantic properties are important to evaluate the validity and reliability of an assurance seal. Therefore, when investigating the effectiveness of assurance seals in online environments the information who protect what and how should be considered and communicated.

Boundaries: P3 also provides some insights on the boundaries of research on CSP selection decision criteria. Extending the research by Saripalli/Pingali (2011) and Repschlaeger et al. (2013), who investigated CSP selection criteria in 2011 and 2013, P3 illustrates temporary boundary under which previous rankings of CSP selection decision are valid. P3 point out how changes in the legal environment, the changing role of IT decision makers, and the ignorance of interdependencies between technical and managerial QoS attributes restrict previous findings to certain point in times.

Further, many studies focus on the perspective of the controlee and investigate if the controlee perceives that the enacted controls are appropriate (Heumann et al. 2015; Remus et al. 2016; Tiwana/Keil 2009). P4 and P5 extend this view by investigating the control perception of a controller with respect to the effectiveness of the controls enacted through control agents. According to our findings, even if controllers have limited resources to control others, additional means of control are available by considering external control agents. Hence, we extend the known literature on control by providing a third dimension “who controls?” which should be considered when investigating enacted controls.

12.2 Contributions to Practice

The overall objective of this thesis is to increase the understanding of how customers select cloud services within a professional environment. Accordingly, this section provides guidelines for new and existing cloud customers, CSPs, and cloud service certification authorities.

Guidelines for new and existing cloud customers.

Identification of the most important QoS attributes. Our results provide a starting point for new cloud customers to identify relevant QoS attributes when making CSP comparisons and during the CSP selection process. Using our results, new cloud customers can compare and select CSP by focusing on the most important technical and managerial QoS attributes. Because our professional panel was not able to reach a strong consensus on the importance of QoS attributes, persons charged with making cloud decisions should adapt this list to better accommodate individual requirements.

Trade-off between managerial and technical QoS. According to our results, the combination of technical and managerial QoS attributes is important during CSP selection to assure future cloud service performance and success. While technical QoS attributes help cloud customers to select the best possible CSP to meet organizational requirements (Wang/Du 2016), managerial QoS attributes verify the capabilities of the CSP, increase predictability in the cloud service exchange relationship, and provide confidence in decision-making (Zhou et al. 2007; Ghosh et al. 2015; Huang/Nicol 2013). As cloud customers need to be confident to conduct optimal CSP selection decisions and not all necessary information for decision-making is available, they use managerial QoS attributes. For example, cloud customers are unable to predict future availability of the cloud service because of a lack of complete information. To assure future availability, cloud customers use contracts including predefined penalties in case the

CSP does not offer the services as stipulated in the contract. The combination of technical and managerial QoS attributes is particularly important to assure future performance and conduct optimal CSP selection decisions (Table 24).

Trend for relevant QoS during CSP selection decision. Existing cloud customers are informed about CSP selection because the relative importance of QoS attributes changed during 2011 and 2015. We identify an increasing importance of managerial QoS related to data protection aspects. Such QoS attributes are “legal compliance”, “geolocation of servers”, “transparency of activities”, and “deployment model.” Such QoS attributes are important to gain confidence on adequate data protection. While the geolocation of a server affects data protection through local laws in place, the transparency of activities helps cloud customers decide whether data protection mechanisms are compliant with legal and internal requirements. Further, the deployment model helps cloud customers to gain confidence about the separation of companies’ data from third-party data. Contrary, we identified a decreasing importance of technical and managerial QoS attributes related to avoidance of a CSPs’ opportunistic behavior. These QoS attributes are “contract”, “control”, and “monitoring”. Because of the standardization of cloud services, contracts become standardized and easy to compare. Cloud customers commonly use communities including other cloud customers to gain insights about the accuracy and quality of possible CSPs. Therefore, in line with new cloud customers, existing cloud customers get an updated guidance during CSP comparison and selection decisions.

Control mechanisms in a cloud environment. Our results assist new and existing cloud customers in different cultures in identifying appropriate controls to assure that a CSP has adequate security and privacy protection in place. While the list of the most important QoS attributes is important when making CSP selection, several managerial QoS attributes can also help cloud customers to control CSP, and therefore their sensitive data, by using contracts, privacy policies, or encryption technologies as personal control mechanisms. Assurance seals and laws enable new and existing cloud customers to use proxy control to protect their sensitive data. Cloud customers use reputational mechanisms to apply collective control mechanism within a professional cloud environment. All three forms help cloud customers to evaluate if a CSP has adequate security and privacy protection in place. Nevertheless, customers from low uncertainty avoidance cultures rely more on their own competence to form privacy perceptions. By contrast, customers from high uncertainty avoidance cultures tend to rely more on reputational mechanisms to form their privacy perceptions.

Guidelines for cloud service providers.

International cooperation. Cooperation with third parties and the cloud customer are important for CSPs. To address cloud customers’ needs such as certain geolocation of services or certification requirements, a CSP needs to cooperate with third parties. Geolocation of services not only influence QoS attributes such as latency but also influences legal compliance requirements of customers (Ramgovind et al. 2010). IaaS providers should consider data centers in different countries, while PaaS and SaaS providers might use different IaaS service providers in different countries if they themselves do not offer an adequate infrastructure. Certification of cloud services needs an endorsement conducted by a third party (Sunyaev/Schneider 2013). CSPs might use such endorsements not only to address customers' needs but also to identify potential improvements through an independent certification authority. Furthermore, CSPs should establish suitable relationships with cloud customers using features such as support possibilities to co-create value. Overall, to address customers' needs, CSPs might consider third parties to address customer compliance, latency, or support requirements, or to extend transparency within their services.

Assurance seal selection. Our results suggest that CSPs can influence perceptions of their customers by implementing assurance seals. Hence, CSPs should consider certification authorities to prove their data protection capabilities. However, not all assurance seals influence the perception of customers in the same manner. Assurance seals are based on different quality levels of an audit and issued from certification authorities with different reputations. CSPs should particular choose assurance seals with a high quality level of an audit like continuous certificates issued from a high reputable certification authority.

Required control mechanisms. Our results provide a better understanding about cloud customers' needs during CSP selection decisions and, therefore, guidance for CSPs regarding required control mechanisms. Cloud customers' demand transparency of CSP' activities, monitoring solutions, and up-to-date certificates. Therefore, CSPs should implement and communicate these mechanisms to satisfy existing cloud customers and as a means of acquiring new customers. As a communication example, CSPs could promote these mechanisms on their webpage to address customers' needs during their CSP selection and control process.

Guidelines for cloud service certification authorities.

Effective form of assurance seals. To be effective, any certification authority need to use a certain strategy to communicate their reputation and quality level of an audit. This thesis shows that the usage of assurance seals combined with an attestation report is one effective example for such a communication strategy. An assurance seal including the certification scope, certification method and certification authority in combination with a certification attestation report is effective in creating a retrieval cue for customers' privacy perception.

13 Future Research

It is impossible for a doctoral dissertation to deal with all phenomena, open questions, and issues of an extensive research area such as cloud sourcing research. Moreover, answering research questions often raises subsequent research issues. Hence, based on the findings and limitations of this thesis, this section presents promising avenues for future cloud sourcing research.

Trade-off between cloud and edge computing. CC provides the advantages by definition of "convenient, on-demand network access to a shared pool of configurable computing resources […] that can be rapidly provisioned and released […]" (Mell/Grance 2011). However, as a consequence of centralized resources, latency problems in particular for real-time applications are crucial. One solution for this problem is the combination of CC and edge computing. However, until now it is unclear how a reliable trade-off between these technologies can be reached. To investigate such a trade-off, multiple case-studies might provide further insights.

Compare professional and end-consumer cloud selection decisions. This thesis focuses on decision makers in a professional cloud environment. However, decision makers serve as representatives in companies, and, therefore, may would act in a different way when they make decisions as individual persons. Since companies like Amazon address multi-groups of customers, both, the decision process of professionals and individuals is important to understand for those. Future research might adopt our findings and verify if these are valid in an end-consumer market as well. Therefore, a comparative study could put light into differences between end-consumer and professional decision makers and provide further guidelines for practice.

Privacy impact on individual, organizational, and national level. Privacy judgements in organizations are influenced by decision makers' properties, e.g., dispositions to privacy, organizational requirements, e.g., policies, and legal rules, e.g., data protection law. However, recent findings focus on single-level to describe how privacy perceptions of decision makers are formed. Developing multi-level theories and reconciling process- and variance-based theories through multi-level research can enhance our understanding about how privacy perceptions are formed.

Interplay between CC and supra-national regulations and policy frameworks. This thesis results demonstrate that the legal environment highly influences the perception of decision makers. This is because, cloud services must fulfill the requirements, e.g., from the newly introduced General Data Protection Regulation (GDPR) in Europe, and, therefore, increase their security and privacy protection capabilities. However, since the technology is changing, not only the technology addresses requirements from the legal environment, also the legal environment (slowly) changes based on emerging technologies. Using cross-population and cross-national comparative research approaches and impact assessment could clarify the interplay between emerging technologies and legal environments.

Impact of security breaches and hacker attacks on decision makers preferences for control mechanisms. Research on CSP selection decision assumes a stable environment, in which e.g., legal changes occur only from time to time in a predictable manner. However, security breaches or hacker attacks are not predictable. In case such an event occurs, decision makers might change their priorities on how they judge privacy or conduct CSP selection decisions. To address this issue, an event study could shed light on such changes.

14 Conclusion

Motivated by the low and different adoption rate of cloud services across countries, the purpose of this thesis was to increase the knowledge about a more nuanced understanding of the cognitive decision-making process as the basis for the success of IT outsourcing and cloud adoption. This thesis contributes to research by addressing four research challenges in the field of IT outsourcing in general, and specifically of cloud sourcing that are not addressed in extant research so far: (1) missing focus on micro-level as unit of analysis, (2) fragmented research on control mechanisms, (3) missing integration of psychological control perspective, and (4) assurance seals are handled as a black box. This thesis contributes to practice by providing guidelines for (potential) cloud customers, CSPs, and certification authorities. Further fruitful avenues for future research comprise among others the privacy impact on individual, organizational, and national level, and an interplay between CC and supra-national regulations and policy frameworks.

References

Adler, M.; Ziglio, E. (1996): Gazing into the oracle: The Delphi method and its application to social policy and public health, Jessica Kingsley Publishers, London 1996.

Agrawal, M.; Kishore, R.; Rao, H.R. (2006): Market reactions to e-business outsourcing announcements: An event study. In: Information & Management, Vol. 43 (2006) No. 7, pp. 861-873.

Akter, S.; D'Ambra, J.; Ray, P. (2010): User perceived service quality of m-health services in developing countries. *European Conference on Information Systems*. Pretoria.

Anderson, N.H. (1971): Integration theory and attitude change. In: Psychological Review, Vol. 78 (1971) No. 3, pp. 171-206.

Anderson, N.H. (1974): Cognitive algebra: Integration theory applied to social attribution. In: Advances in Experimental Social Psychology, Vol. 7 (1974), pp. 1-101.

Anderson, N.H. (1981): Foundations of information integration theory, Academic Press, New York 1981.

Anderson, R.; Moore, T. (2006): The economics of information security. In: Science, Vol. 314 (2006) No. 5799, pp. 610-613.

Andriole, S.J. (2007): Mining for digital gold: technology due diligence for CIOs. In: Communications of the Association for Information Systems, Vol. 20 (2007) No. 1, pp. 371-381.

Ang, S.; Cummings, L.L. (1997): Strategic response to institutional influences on information systems outsourcing. In: Organization Science, Vol. 8 (1997) No. 3, pp. 235-256.

Anisetti, M.; Ardagna, C.; Damiani, E.; El Ioini, N.; Gaudenzi, F. (2017): Modeling time, probability, and configuration constraints for continuous cloud service certification. In: Computers & Security, Vol. 72 (2017), pp. 234-254.

Ariely, D.; Norton, M.I. (2007): Psychology and experimental economics: A gap in abstraction. In: Current Directions in Psychological Science, Vol. 16 (2007) No. 6, pp. 336-339.

Armbrust, M.; Fox, A.; Griffith, R.; Joseph, A.D.; Katz, R.; Konwinski, A.; Lee, G.; Patterson, D.; Rabkin, A.; Stoica, I. (2010): A view of cloud computing. In: Communications of the ACM, Vol. 53 (2010) No. 4, pp. 50-58.

Aubert, B.A.; Houde, J.-F.; Patry, M.; Rivard, S. (2012): A multi-level investigation of information technology outsourcing. In: The Journal of Strategic Information Systems, Vol. 21 (2012) No. 3, pp. 233-244.

Axelrod, R.; Hamilton, W.D. (1981): The Evolution of Cooperation. In: Science, Vol. 211 (1981) No. 4489, pp. 1390-1396.

Ba, S.; Pavlou, P.A. (2002): Evidence of the effect of trust building technology in electronic markets: Price premiums and buyer behavior. In: Management Information Systems Quarterly, Vol. 26 (2002) No. 3, pp. 243-268.

Babbie, E.R. (1973): Survey research methods, Wadsworth 1973.

Bandura, A. (2001): Social cognitive theory: An agentic perspective. In: Annual Review of Psychology, Vol. 52 (2001) No. 1, pp. 1-26.

Bansal, G.; Zahedi, F. (2008): The moderating influence of privacy concern on the efficacy of privacy assurance mechanisms for building trust: A multiple-context investigation. *International Conference on Information Systems* (pp. 7). Paris.

Bansal, G.; Zahedi, F.; Gefen, D. (2015): The role of privacy assurance mechanisms in building trust and the moderating role of privacy concern. In: European Journal of Information Systems, Vol. 24 (2015) No. 2015, pp. 624-644.

Barber, B. (1983): The logic and limits of trust, Rutgers University Press, New Brunswick 1983.

Barzel, Y. (1982): Measurement cost and the organization of markets. In: Journal of Law & Economics, Vol. 25 (1982) No. 1, pp. 27-48.

Bélanger, F.; Crossler, R.E. (2011): Privacy in the digital age: a review of information privacy research in information systems. In: Management Information Systems Quarterly, Vol. 35 (2011) No. 4, pp. 1017-1042.

Benassi, P. (1999): TRUSTe: an online privacy seal program. In: Communications of the ACM, Vol. 42 (1999) No. 2, pp. 56-59.

Benlian, A. (2009): A transaction cost theoretical analysis of software-as-a-service (SAAS)-based sourcing in SMBs and enterprises. *European Conference on Information Systems* (pp. 25-36). Verona.

Benlian, A.; Hess, T. (2011): Opportunities and risks of software-as-a-service: Findings from a survey of IT executives. In: Decision Support Systems, Vol. 52 (2011) No. 1, pp. 232-246.

Benlian, A.; Hess, T.; Buxmann, P. (2009): Drivers of SaaS-adoption–an empirical study of different application types. In: Business & Information Systems Engineering, Vol. 1 (2009) No. 5, pp. 357-369.

Berry, D.; Hayward, B.; Heneghan, L.; Snyder, M.E.; Tjon, G. (2016): Clouds on the horizon. KPMG, 2016.

Bhattacherjee, A. (2012): Social science research: Principles, methods, and practices 2012.

Bhattacherjee, A.; Park, S.C. (2014): Why end-users move to the cloud: a migration-theoretic analysis. In: European Journal of Information Systems, Vol. 23 (2014) No. 3, pp. 357-372.

Blaskovich, J.; Mintchik, N. (2011): Accounting executives and IT outsourcing recommendations: an experimental study of the effect of CIO skills and institutional isomorphism. In: Journal of Information Technology, Vol. 26 (2011) No. 2, pp. 139-152.

Böhm, M.; Koleva, G.; Leimeister, S.; Riedl, C.; Krcmar, H. (2010): Towards a generic value network for cloud computing. In: International Workshop on Grid Economics and Business Models. Eds. Springer, Berlin Heidelberg 2010, pp. 129-140.

Böhm, M.; Leimeister, S.; Riedl, C.; Krcmar, H. (2009): Cloud Computing: Outsourcing 2.0 oder ein neues Geschäftsmodell zur Bereitstellung von IT-Ressourcen. In: Information Management & Consulting, Vol. 24 (2009) No. 2, pp. 6-14.

Brender, N.; Markov, I. (2013): Risk perception and risk management in cloud computing: Results from a case study of Swiss companies. In: International Journal of Information Management, Vol. 33 (2013) No. 5, pp. 726-733.

Bria, A.; Gessler, F.; Queseth, O.; Stridh, R.; Unbehaun, M.; Wu, J.; Zander, J.; Flament, M. (2001): 4th-generation wireless infrastructures: scenarios and research challenges. In: IEEE Personal Communications, Vol. 8 (2001) No. 6, pp. 25-31.

Burt, R.S. (2009): Structural holes: The social structure of competition, Harvard university press 2009.

Burton-Jones, A.; Straub, D.W. (2006): Reconceptualizing system usage: An approach and empirical test. In: Information Systems Research, Vol. 17 (2006) No. 3, pp. 228-246.

Cayirci, E.; Garaga, A.; de Oliveira, A.S.; Roudier, Y. (2016): A risk assessment model for selecting cloud service providers. In: Journal of Cloud Computing, Vol. 5 (2016) No. 1, pp. 14.

Chae, H.-C.; Koh, C.E.; Prybutok, V.R. (2014): Information technology capability and firm performance: contradictory findings and their possible causes. In: Management Information Systems Quarterly, Vol. 38 (2014) No. 1, pp. 305-326.

Chandra, S.; Theng, Y.L.; Lwin, M.O.; Foo, S.S.-B. (2010): Understanding collaborations in virtual world. *Pacific Asia Conference on Information Systems* (pp. 96). Taipei.

Chang, S.-I.; Yen, D.C.; Ng, C.S.-P.; Chang, W.-T. (2012): An analysis of IT/IS outsourcing provider selection for small-and medium-sized enterprises in Taiwan. In: Information & Management, Vol. 49 (2012) No. 5, pp. 199-209.

Chellappa, R.K. (2008): Consumers' trust in electronic commerce transactions: the role of perceived privacy and perceived security. Emory University, Atlanta, GA.

Chen, C.C.; Mitchell, A. (2010): Improving the trust of users on social networking sites via self-construal traits. *Americas Conference on Information Systems* (pp. 5). Lima.

Chen, P.-y.; Wu, S.-y. (2013): The impact and implications of on-demand services on market structure. In: Information Systems Research, Vol. 24 (2013) No. 3, pp. 750-767.

Chen, Y.-H.; Chien, S.-H. (2009): Investigating factors influencing the use of e-government service. *Americas Conference on Information Systems* (pp. 695). San Francisco.

Cherryholmes, C.H. (1992): Notes on pragmatism and scientific realism. In: Educational Researcher, Vol. 21 (1992) No. 6, pp. 13-17.

Chua, W.F. (1986): Radical developments in accounting thought. In: Accounting Review, Vol. 61 (1986) No. 4, pp. 601-632.

Clemons, E.K.; Hitt, L.M. (2004): Poaching and the misappropriation of information: Transaction risks of information exchange. In: Journal of Management Information Systems, Vol. 21 (2004) No. 2, pp. 87-107.

Cohen, J. (1992): A power primer. In: Psychological Bulletin, Vol. 112 (1992) No. 1, pp. 155-159.

Cohen, L.; Manion, L.; Morrison, K. (2013): Research methods in education (Vol. 6), Routledge, London 2013.

Cooper, D.R.; Emory, C.W. (1995): Business Research Methods, IRWIN, Chicago 1995.

Cooper, H.M. (1988): Organizing knowledge syntheses: A taxonomy of literature reviews. In: Knowledge, Technology & Policy, Vol. 1 (1988) No. 1, pp. 104-126.

Creswell, J. (2009): Research design: Qualitative, quantitative, and mixed methods approaches, SAGE Publications, Los Angeles 2009.

CSA (2016): The Treacherous 12. Cloud Security Alliance, 2016.

Culnan, M.J.; Armstrong, P.K. (1999): Information privacy concerns, procedural fairness, and impersonal trust: An empirical investigation. In: Organization Science, Vol. 10 (1999) No. 1, pp. 104-115.

Culnan, M.J.; Bies, R.J. (2003): Consumer privacy: Balancing economic and justice considerations. In: Journal of Social Issues, Vol. 59 (2003) No. 2, pp. 323-342.

Currie, W.; Seddon, J. (2014): A cross-country study of cloud computing policy and regulation in healthcare. *European Conference on Information Systems*. Tel Aviv.

Dalkey, N.; Helmer, O. (1963): An experimental application of the Delphi method to the use of experts. In: Management Science, Vol. 9 (1963) No. 3, pp. 458-467.

De Charms, R. (2013): Personal causation: The internal affective determinants of behavior, Routledge, New York 2013.

Detert, J.R.; Treviño, L.K.; Sweitzer, V.L. (2008): Moral disengagement in ethical decision making: A study of antecedents and outcomes. In: Journal of Applied Psychology, Vol. 93 (2008) No. 2, pp. 374-391.

Devaraj, S.; Fan, M.; Kohli, R. (2002): Antecedents of B2C channel satisfaction and preference: validating e-commerce metrics. In: Information systems research, Vol. 13 (2002) No. 3, pp. 316-333.

Dibbern, J.; Winkler, J.; Heinzl, A. (2008): Explaining variations in client extra costs between software projects offshored to India. In: Management Information Systems Quarterly, Vol. 32 (2008) No. 2, pp. 333-366.

Dimoka, A.; Hong, Y.; Pavlou, P.A. (2012): On product uncertainty in online markets: Theory and evidence. In: Management Information Systems Quarterly, Vol. 36 (2012).

Dinev, T.; Bellotto, M.; Hart, P.; Russo, V.; Serra, I.; Colautti, C. (2006): Privacy calculus model in e-commerce–a study of Italy and the United States. In: European Journal of Information Systems, Vol. 15 (2006) No. 4, pp. 389-402.

Dinev, T.; Goo, J.; Hu, Q.; Nam, K. (2009): User behaviour towards protective information technologies: the role of national cultural differences. In: Information Systems Journal, Vol. 19 (2009) No. 4, pp. 391-412.

Dinev, T.; Xu, H.; Smith, J.H.; Hart, P. (2013): Information privacy and correlates: an empirical attempt to bridge and distinguish privacy-related concepts. In: European Journal of Information Systems, Vol. 22 (2013) No. 3, pp. 295-316.

Doney, P.M.; Cannon, J.P. (1997): An examination of the nature of trust in buyer-seller relationships. In: Journal of Marketing, Vol. 61 (1997) No. 2, pp. 35-51.

Doney, P.M.; Cannon, J.P.; Mullen, M.R. (1998): Understanding the influence of national culture on the development of trust. In: Academy of Management Review, Vol. 23 (1998) No. 3, pp. 601-620.

Dongus, K.; Yetton, P.; Schermann, M.; Krcmar, H. (2014): Transaction Cost Economics and Industry Maturity in It Outsourcing: A Meta-Analysis of Contract Type Choice. Paper presented at the Proceedings of the European Conference on Information Systems (ECIS) 2014, Tel Aviv, Israel.

Dove, E.S.; Joly, Y.; Tassé, A.-M.; in Genomics, P.P.P.; Committee, S.P.G.I.S.; Knoppers, B.M.; Consortium, I.C.G.; Ethics; Committee, P. (2015): Genomic cloud computing: legal and ethical points to consider. In: European Journal of Human Genetics, Vol. 23 (2015) No. 10, pp. 1271-1278.

Du, S.; Keil, M.; Mathiassen, L.; Shen, Y.; Tiwana, A. (2007): Attention-shaping tools, expertise, and perceived control in IT project risk assessment. In: Decision Support Systems, Vol. 43 (2007) No. 1, pp. 269-283.

Dyer, J.H. (1997): Effective interfirm collaboration: How firms minimize transaction costs and maximize transaction value. In: Strategic Management Journal, Vol. 18 (1997) No. 7, pp. 535-556.

El Zant, B.; Gagnaire, M. (2015): Towards a unified customer aware figure of merit for CSP selection. In: Journal of Cloud Computing, Vol. 4 (2015) No. 24, pp. 1-23.

Fromkin, H.L.; Streufert, S. (1976): Laboratory experimentation 1976.

Frye, N.E.; Dornisch, M.M. (2010): When is trust not enough? The role of perceived privacy of communication tools in comfort with self-disclosure. In: Computers in Human Behavior, Vol. 26 (2010) No. 5, pp. 1120-1127.

Galanxhi, H.; Nah, F.F.H. (2006): Privacy issues in the era of ubiquitous commerce. In: Electronic Markets, Vol. 16 (2006) No. 3, pp. 222-232.

Galer, S. (2015): Top Ten 2016 IT Market Predictions. http://www.digitalistmag.com/technologies/2015/11/13/idc-releases-top-ten-2016-it-market-predictions-03746307, accessed at 22.11.2015.2015.

Gallupe, R.B.; Bastianutti, L.M.; Cooper, W.H. (1991): Unblocking brainstorms. In: Journal of Applied Psychology, Vol. 76 (1991) No. 1, pp. 137-142.

Gao, G.; Gopal, A.; Agarwal, R. (2010): Contingent effects of quality signaling: evidence from the Indian offshore IT services industry. In: Management Science, Vol. 56 (2010) No. 6, pp. 1012-1029.

Garg, S.K.; Versteeg, S.; Buyya, R. (2013): A framework for ranking of cloud computing services. In: Future Generation Computer Systems, Vol. 29 (2013) No. 4, pp. 1012-1023.

Garrison, G.; Kim, S.; Wakefield, R.L. (2012): Success factors for deploying cloud computing. In: Communications of the ACM, Vol. 55 (2012) No. 9, pp. 62-68.

Garrison, G.; Wakefield, R.L.; Kim, S. (2015): The effects of IT capabilities and delivery model on cloud computing success and firm performance for cloud supported processes and operations. In: International Journal of Information Management, Vol. 35 (2015) No. 4, pp. 377-393.

Gartner (2015): Forecast Analysis: Public Cloud Services, Worldwide, 1Q15 Update. https://www.gartner.com/doc/3077621/forecast-analysis-public-cloud-services, accessed at 18.11.2015.2015.

Gefen, D.; Karahanna, E.; Straub, D.W. (2003): Inexperience and experience with online stores: The importance of TAM and trust. In: IEEE Transactions on Engineering Management, Vol. 50 (2003) No. 3, pp. 307-321.

Ghafori, V.; Sarhadi, R.M. (2013): Best cloud provider selection using integrated ANP-DEMATEL and prioritizing SMI attributes. In: International Journal of Computer Applications, Vol. 71 (2013) No. 16, pp. 18-25.

Ghosh, N.; Ghosh, S.K.; Das, S.K. (2015): SelCSP: A framework to facilitate selection of cloud service providers. In: IEEE Transactions on Cloud Computing, Vol. 3 (2015) No. 1, pp. 66-79.

Giannakouris, K.; Smihily, M. (2016): Cloud computing - statistics on the use by enterprises. Eurostat, 2016.

Godse, M.; Mulik, S. (2009): An approach for selecting software-as-a-service (SaaS) product. *IEEE International Conference on Cloud Computing* (pp. 155-158). Los Angeles: IEEE.

Goodman, S. (2000): Protecting privacy in a b2b world. In: Mortgage Banking, Vol. 60 (2000) No. 7, pp. 83-87.

Gopal, A.; Koka, B.R. (2012): The asymmetric benefits of relational flexibility: Evidence from software development outsourcing. In: Management Information Systems Quarterly, Vol. 36 (2012) No. 2, pp. 553-576.

Gordon, T.J.; Helmer, O. (1964): Report on a long-range forecasting study. Rand Corporation Santa Monica, CA, 1964.

Gravetter, F.J.; Forzano, L.-A.B. (2003): Research methods for the behavioral sciences, Cengage, Boston 2003.

Gregory, R.W.; Keil, M. (2014): Blending bureaucratic and collaborative management styles to achieve control ambidexterity in IS projects. In: European Journal of Information Systems, Vol. 23 (2014) No. 3, pp. 343-356.

Guba, E.G.; Lincoln, Y.S. (1994): Competing paradigms in qualitative research (Vol. 2), Sage, Thousand Oaks 1994.

Gundlach, G.T.; Cannon, J.P. (2010): "Trust but verify"? The performance implications of verification strategies in trusting relationships. In: Journal of the Academy of Marketing Science, Vol. 38 (2010) No. 4, pp. 399-417.

Gupta, A.; Kannan, K.; Sanyal, P. (Forthcoming 2018): Economic Experiments in Information Systems. In: Management Information Systems Quarterly, (Forthcoming 2018).

Gupta, P.; Seetharaman, A.; Raj, J.R. (2013): The usage and adoption of cloud computing by small and medium businesses. In: International Journal of Information Management, Vol. 33 (2013) No. 5, pp. 861-874.

Gurbaxani, V.; Whang, S. (1991): The impact of information systems on organizations and markets. In: Communications of the ACM, Vol. 34 (1991) No. 1, pp. 59-73.

Häder, M.; Häder, S. (1994): Die Grundlagen der Delphi-Methode: Ein Literaturbericht. Mannheim.

Han, J.-S.; Lee, S.-Y.T. (2012): Impact of Vendor Selection on Firms' IT Outsourcing: The Korea Experience. In: Journal of Global Information Management, Vol. 20 (2012) No. 2, pp. 25-43.

Heart, T. (2010): Who is out there?: exploring the effects of trust and perceived risk on saas adoption intentions. In: ACM SIGMIS Database: the DATABASE for Advances in Information Systems, Vol. 41 (2010) No. 3, pp. 49-68.

Heidkamp, P.; Pols, A. (2017): Cloud-Monitor 2017. KPMG AG, 2017.

Henderson, J.C.; Lee, S. (1992): Managing I/S design teams: a control theories perspective. In: Management Science, Vol. 38 (1992) No. 6, pp. 757-777.

Heumann, J.; Wiener, M.; Remus, U.; Mähring, M. (2015): To coerce or to enable? Exercising formal control in a large information systems project. In: Journal of Information Technology, Vol. 30 (2015) No. 4, pp. 337-351.

Hirschheim, R. (1985): Information systems epistemology: An historical perspective. In: Research methods in information systems. Eds.: Mumford, E.; Hurshheim, R.; Fitzgerald, G.; Wood Harper, T., Amsterdam 1985, pp. 13-35.

Hoadley, C.M.; Xu, H.; Lee, J.J.; Rosson, M.B. (2010): Privacy as information access and illusory control: The case of the Facebook News Feed privacy outcry. In: Electronic Commerce Research and Applications, Vol. 9 (2010) No. 1, pp. 50-60.

Hofstede, G. (2011): Dimensionalizing cultures: The Hofstede model in context. In: Online readings in psychology and culture, Vol. 2 (2011) No. 1, pp. 1-26.

Hossain, M.M.; Prybutok, V.R. (2008): Consumer acceptance of RFID technology: An exploratory study. In: IEEE Transactions on Engineering Management, Vol. 55 (2008) No. 2, pp. 316-328.

House, R.J.; Hanges, P.J.; Javidan, M.; Dorfman, P.W.; Gupta, V. (2004): Culture, leadership, and organizations, Sage publications, London 2004.

Hu, X.; Wu, G.; Wu, Y.; Zhang, H. (2010): The effects of Web assurance seals on consumers' initial trust in an online vendor: A functional perspective. In: Decision Support Systems, Vol. 48 (2010) No. 2, pp. 407-418.

Huang, J.; Nicol, D.M. (2013): Trust mechanisms for cloud computing. In: Journal of Cloud Computing: Advances, Systems and Applications, Vol. 2 (2013) No. 9, pp. 1-14.

Huang, L.-T.; Farn, C.-K.; Yin, K.-L. (2005): On initial trust building for ecommerce: Revisiting from the perspective of signal theory and trust transference. *European Conference on Information Systems* (pp. 94). Regensburg.

Hui, K.-L.; Teo, H.H.; Lee, S.-Y.T. (2007): The value of privacy assurance: An exploratory field experiment. In: Management Information Systems Quarterly, Vol. 31 (2007) No. 1, pp. 19-33.

Iivari, J.; Hirschheim, R.; Klein, H.K. (2004): Towards a distinctive body of knowledge for Information Systems experts: coding ISD process knowledge in two IS journals. In: Information systems journal, Vol. 14 (2004) No. 4, pp. 313-342.

Isaac, S.; Michael, W.B. (1995): Handbook in research and evaluation: A collection of principles, methods, and strategies useful in the planning, design, and evaluation of studies in education and the behavioral sciences, Edits publishers, San Diego 1995.

Jain, A.; Thietart, R.-A. (2013): Knowledge based transactions and decision framing in Information Technology Outsourcing. In: The Journal of Strategic Information Systems, Vol. 22 (2013) No. 4, pp. 315-327.

Johnson, C.A. (1974): Privacy as personal control, Environmental Design Research Association, Washington, DC 1974.

Johnson, R.B.; Onwuegbuzie, A.J.; Turner, L.A. (2007): Toward a definition of mixed methods research. In: Journal of mixed methods research, Vol. 1 (2007) No. 2, pp. 112-133.

Johnston, A.C.; Warkentin, M. (2010): Fear appeals and information security behaviors: an empirical study. In: Management Information Systems Quarterly, Vol. 34 (2010) No. 3, pp. 549-566.

Kahneman, D.; Tversky, A. (1979): Prospect theory: An analysis of decision under risk. In: Econometrica, Vol. 47 (1979) No. 2, pp. 263-291.

Kaisler, S.; Money, W.H.; Cohen, S.J. (2012): A decision framework for cloud computing. Paper presented at the Hawaii International Conference on System Science (HICSS), 2012 Maui, USA, pp. 1553-1562.

Karunagaran, S.; Mathew, S.; Lehner, F. (2016): Differential adoption of cloud technology: A multiple case study of large firms and SMEs. *International Conference on Information Systems*. Doublin.

Keil, M.; Tan, B.C.; Wei, K.-K.; Saarinen, T.; Tuunainen, V.; Wassenaar, A. (2000): A cross-cultural study on escalation of commitment behavior in software projects. In: Management Information Systems Quarterly, Vol. 24 (2000) No. 2, pp. 299-325.

Keith, M.J.; Babb Jr, J.S.; Furner, C.P.; Abdullat, A. (2010): Privacy assurance and network effects in the adoption of location-based services: An iPhone experiment. *International Conference on Information Systems* (pp. 237). St. Louis.

Keith, M.J.; Babb Jr, J.S.; Furner, C.P.; Abdullat, A. (2011): The role of mobile self-efficacy in the adoption of location-based applications: An iPhone experiment. *Hawaii International Conference on System Sciences* (pp. 1-10). Manoa: IEEE.

Keith, M.J.; Babb, J.S.; Lowry, P.B.; Furner, C.P.; Abdullat, A. (2015): The role of mobile-computing self-efficacy in consumer information disclosure. In: Information Systems Journal, Vol. 25 (2015) No. 6, pp. 637-667.

Kendall, J.W. (1977): Variations of delphi. In: Technological Forecasting and Social Change, Vol. 11 (1977) No. 1, pp. 75-85.

Keppel, G. (1991): Design and analysis: A researcher's handbook (Vol. 3), Prentice-Hall, Inc, Englewood Cliffs 1991.

Khazanchi, D.; Sutton, S.G. (2001): Assurance services for business-to-business electronic commerce: a framework and implications. In: Journal of the Association for Information Systems, Vol. 1 (2001) No. 1, pp. 11.

Kim, D.; Benbasat, I. (2006): The effects of trust-assuring arguments on consumer trust in Internet stores: Application of Toulmin's model of argumentation. In: Information Systems Research, Vol. 17 (2006) No. 3, pp. 286-300.

Kim, D.; Benbasat, I. (2009): Trust-assuring arguments in B2C e-commerce: Impact of content, source, and price on trust. In: Journal of Management Information Systems, Vol. 26 (2009) No. 3, pp. 175-206.

Kim, D.; Koohikamali, M. (2015): Does information sensitivity make a difference? Mobile applications’ privacy statements: A text mining approach. *Americas Conference on Information Systems*. Savannah.

Kim, D.J. (2008): Self-perception-based versus transference-based trust determinants in computer-mediated transactions: A cross-cultural comparison study. In: Journal of Management Information Systems, Vol. 24 (2008) No. 4, pp. 13-45.

Kim, D.J.; Sivasailam, N.; Rao, H.R. (2004): Information assurance in B2C websites for information goods/services. In: Electronic Markets, Vol. 14 (2004) No. 4, pp. 344-359.

Kim, D.J.; Yim, M.-S.; Sugumaran, V.; Rao, H.R. (2015): Web assurance seal services, trust and consumers’ concerns: An investigation of e-commerce transaction intentions across two nations. In: European Journal of Information Systems, Vol. 25 (2015) No. 3, pp. 252-273.

Kimery, K.M.; McCord, M. (2002a): Third-party assurances: Mapping the road to trust in e-retailing. In: Journal of Information Technology Theory and Application, Vol. 4 (2002a) No. 2, pp. 63-82.

Kimery, K.M.; McCord, M. (2002b): Third-party assurances: The road to trust in online retailing. *Hawaii International Conference on System Sciences* (pp. 10 pp.). Big Island: IEEE.

Kirk, R.E. (1982): Experimental design, John Wiley & Sons, Inc., Published Online 1982.

Kirsch, L.S. (1997): Portfolios of control modes and IS project management. In: Information Systems Research, Vol. 8 (1997) No. 3, pp. 215-239.

Ko, D.-G.; Kirsch, L.J.; King, W.R. (2005): Antecedents of knowledge transfer from consultants to clients in enterprise system implementations. In: Management Information Systems Quarterly, Vol. 29 (2005) No. 1, pp. 59-85.

Koehler, P.; Anandasivam, A.; Dan, M.; Weinhardt, C. (2010): Customer heterogeneity and tariff biases in cloud computing. *International Conference on Information Systems* (pp. 106). St. Louis.

Koh, T.K.; Fichman, M.; Kraut, R.E. (2012): Trust across borders: buyer-supplier trust in global business-to-business e-commerce. In: Journal of the Association for Information Systems, Vol. 13 (2012) No. 11, pp. 886-922.

Kourtesis, D.; Bratanis, K.; Friesen, A.; Verginadis, Y.; Simons, A.J.; Rossini, A.; Schwichtenberg, A.; Gouvas, P. (2014): Brokerage for Quality Assurance and Optimisation of Cloud Services: An Analysis of Key Requirements. *Service-Oriented Computing – ICSOC 2013 Workshops* (pp. 150-162): Springer.

KPMG, A. (2015): Cloud Monitor 2015. Cloud-Computing in Deutschland – Status quo und Perspektiven. KPMG AG, 2015.

Kraemer, K.; Dutton, W. (1991): Survey research in the study of management information systems. *The information systems research challenge: Survey research methods* (Vol. 3, pp. 3-58): Harvard Business School Press.

Krasnova, H.; Veltri, N.F. (2010): Privacy calculus on social networking sites: Explorative evidence from Germany and USA. *Hawaii international conference on System Sciences* (pp. 1-10). Koloa: IEEE.

Kritikos, K.; Plexousakis, D. (2009): Mixed-integer programming for QoS-based web service matchmaking. In: IEEE Transactions on Services Computing, Vol. 2 (2009) No. 2, pp. 122-139.

Kuan, H.-H.; Bock, G.-W. (2005): An exploratory study of before-interaction trust transference in multichannel retailers. *International Conference on Information Systems* (pp. 60). Las Vegas.

Kung, L.; Kung Dr, H.-J. (2013): Environmental pressure on software as a service adoption: An integrated perspective. *Americas Conference on Information Systems*. Chicago.

Lacity, M.C.; Khan, S.; Yan, A.; Willcocks, L.P. (2010): A review of the IT outsourcing empirical literature and future research directions. In: Journal of Information technology, Vol. 25 (2010) No. 4, pp. 395-433.

Lala, V.; Arnold, V.; Sutton, S.G.; Guan, L. (2002): The impact of relative information quality of e-commerce assurance seals on Internet purchasing behavior. In: International Journal of Accounting Information Systems, Vol. 3 (2002) No. 4, pp. 237-253.

Lang, M.; Wiesche, M.; Krcmar, H. (2016): What are the most important criteria for cloud service provider selection? A Delphi study. *European Conference on Information Systems*. Istanbul.

Lang, M.; Wiesche, M.; Krcmar, H. (2017): Conceptualization of Relational Assurance Mechanisms - A Literature Review on Relational Assurance Mechanisms, Their Antecedents and Effects. *International Conference on Wirtschaftsinformatik*. St. Gallen.

Lang, M.; Wiesche, M.; Krcmar, H. (2018a): Criteria for Selecting Cloud Service Providers: A Delphi Study of Quality-of-Service Attributes. In: Information & Management, (2018a).

Lang, M.; Wiesche, M.; Krcmar, H. (2018b): Perceived Control and Privacy in a Professional Cloud Environment. Paper presented at the Hawaii International Conference on System Sciences, Big Island, Hawaii.

Langer, E.J. (1975): The illusion of control. In: Journal of Personality and Social Psychology, Vol. 32 (1975) No. 2, pp. 311.

Lankton, N.; McKnight, D.H.; Thatcher, J.B. (2014): Incorporating trust-in-technology into Expectation Disconfirmation Theory. In: The Journal of Strategic Information Systems, Vol. 23 (2014) No. 2, pp. 128-145.

Lansing, J.; Sunyaev, A.; Benlian, A. (2018): 'Unblackboxing Decision Makers' Interpretations of IS Certifications in the Context of Cloud Service Certifications. In: Journal of the Association for Information Systems, Vol. forthcoming (2018).

Latané, B.; Darley, J.M. (1970): The unresponsive bystander: Why doesn't he help?, Prentice Hall, New York 1970.

Lee, C.H.; Geng, X.; Raghunathan, S. (2013a): Contracting information security in the presence of double moral hazard. In: Information Systems Research, Vol. 24 (2013a) No. 2, pp. 295-311.

Lee, S.-G.; Chae, S.H.; Cho, K.M. (2013b): Drivers and inhibitors of SaaS adoption in Korea. In: International Journal of Information Management, Vol. 33 (2013b) No. 3, pp. 429-440.

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

Levy, Y.; Ellis, T.J. (2006): A systems approach to conduct an effective literature review in support of information systems research. In: Informing Science, Vol. 9 (2006).

Li, E.Y.; Yen, H.R.; Liu, C.-C.; Chang, L.F. (2013): From structural assurances to trusting beliefs: Validating persuasion principles in the context of online shopping. *Pacific Asia Conference on Information Systems* (pp. 127). Jeju Island.

Lian, J.-W.; Yen, D.C.; Wang, Y.-T. (2014): An exploratory study to understand the critical factors affecting the decision to adopt cloud computing in Taiwan hospital. In: International Journal of Information Management, Vol. 34 (2014) No. 1, pp. 28-36.

Liang, H.; Wang, J.-J.; Xue, Y.; Cui, X. (2015): IT Outsourcing Research from 1992 to 2013: A Literature Review Based on Main Path Analysis. In: Information & Management, (2015).

Liao, Z. (2005): Trust building and sustainable internet banking. *Americas Conference on Information Systems* (pp. 16). Omaha.

Lichtenstein, S.; Slovic, P. (1973): Response-induced reversals of preference in gambling: An extended replication in Las Vegas. In: Journal of Experimental Psychology, Vol. 101 (1973) No. 1, pp. 16-20.

Lin, A.; Chen, N.-C. (2012): Cloud computing as an innovation: Percepetion, attitude, and adoption. In: International Journal of Information Management, Vol. 32 (2012) No. 6, pp. 533-540.

Lins, S.; Schneider, S.; Sunyaev, A. (2016): Trust is good, control is better: Creating secure clouds by continuous auditing. In: IEEE Transactions on Cloud Computing, Vol. PP (2016) No. 99.

Lins, S.; Sunyaev, A. (2017): Unblackboxing IT Certifications: A Theoretical Model Explaining IT Certification Effectiveness. Paper presented at the International Conference on Information Systems, Soul.

Linstone, H.A.; Turoff, M. (1975): The Delphi method: Techniques and applications (Vol. 29), Addison-Wesley Publishing, Boston, USA 1975.

Loh, L.; Venkatraman, N. (1992): Diffusion of information technology outsourcing: influence sources and the Kodak effect. In: Information Systems Research, Vol. 3 (1992) No. 4, pp. 334-358.

Low, C.; Chen, Y.; Wu, M. (2011): Understanding the determinants of cloud computing adoption. In: Industrial Management & Data Systems, Vol. 111 (2011) No. 7, pp. 1006-1023.

Lowry, P.B.; Moody, G.; Vance, A.; Jensen, M.; Jenkins, J.; Wells, T. (2012): Using an elaboration likelihood approach to better understand the persuasiveness of website privacy assurance cues for online consumers. In: Journal of the American Society for Information Science and Technology, Vol. 63 (2012) No. 4, pp. 755-776.

Lowry, P.B.; Posey, C.; Bennett, R.B.J.; Roberts, T.L. (2015): Leveraging fairness and reactance theories to deter reactive computer abuse following enhanced organisational information security policies: An empirical study of the influence of counterfactual reasoning and organisational trust. In: Information Systems Journal, Vol. 25 (2015) No. 3, pp. 193-273.

Lowry, P.B.; Vance, A.; Moody, G.; Beckman, B.; Read, A. (2008): Explaining and predicting the impact of branding alliances and web site quality on initial consumer trust of e-commerce web sites. In: Journal of Management Information Systems, Vol. 24 (2008) No. 4, pp. 199-224.

Lübbecke, P.; Lackes, R. (2015): Drivers and Inhibitors for the Adoption of Public Cloud Services–an Empirical Study. *Twenty-first Americas Conference on Information Systems*. Puerto Rico.

Luftman, J.D., Barry; Dwivedi, R.; Santana, M.; Zadeh, H.S.; Rigoni, E. (2015): Influential IT Management Trends: An International Study. In: Journal of Information Technology, Vol. 30 (2015) No. 3, pp. 293-305.

Luoma, E.; Nyberg, T. (2011): Four scenarios for adoption of cloud computing in china. *European Conference on Information Systems*. Helsinki.

MacKenzie, S.B.; Podsakoff, P.M.; Podsakoff, N.P. (2011): Construct measurement and validation procedures in MIS and behavioral research: Integrating new and existing techniques. In: Management Information Systems Quarterly, Vol. 35 (2011) No. 2, pp. 293-334.

Mäntymäki, M. (2008): Exploring customers' post-adoption perceptions: A study on trust, commitment and related constructs in B2C online service context. *Pacific Asia Conference on Information Systems* (pp. 216). Suzhou.

Margulis, S.T. (2003): Privacy as a social issue and behavioral concept. In: Journal of Social Issues, Vol. 59 (2003) No. 2, pp. 243-261.

McKnight, D.H.; Choudhury, V.; Kacmar, C. (2002a): Developing and validating trust measures for e-commerce: An integrative typology. In: Information Systems Research, Vol. 13 (2002a) No. 3, pp. 334-359.

McKnight, D.H.; Choudhury, V.; Kacmar, C. (2002b): The impact of initial consumer trust on intentions to transact with a web site: a trust building model. In: The Journal of Strategic Information Systems, Vol. 11 (2002b) No. 3, pp. 297-323.

McKnight, D.H.; Cummings, L.L.; Chervany, N.L. (1998): Initial trust formation in new organizational relationships. In: Academy of Management Review, Vol. 23 (1998) No. 3, pp. 473-490.

Meiseberg, B. (2015): Linkages among Trust, Monitoring & Performance in Interfirm Relationships: A Cross-National Study. Paper presented at the Academy of Management Proceedings, Vancouver, Canada.

Mell, P.; Grance, T. (2011): The NIST definition of cloud computing. National Institute of Standards and Technology, 2011.

Menzel, M.; Ranjan, R.; Wang, L.; Khan, S.U.; Chen, J. (2015): CloudGenius: A hybrid decision support method for automating the migration of web application clusters to public clouds. In: IEEE Transactions on Computers, Vol. 64 (2015) No. 5, pp. 1336-1348.

Messerschmidt, C.M.; Hinz, O. (2013): Explaining the adoption of grid computing: An integrated institutional theory and organizational capability approach. In: The Journal of Strategic Information Systems, Vol. 22 (2013) No. 2, pp. 137-156.

Michell, V.; Fitzgerald, G. (1997): The IT outsourcing market-place: vendors and their selection. In: Journal of Information Technology, Vol. 12 (1997) No. 3, pp. 223-237.

Milne, G.R.; Culnan, M.J. (2004): Strategies for reducing online privacy risks: Why consumers read (or don't read) online privacy notices. In: Journal of Interactive Marketing, Vol. 18 (2004) No. 3, pp. 15-29.

Moe, C.E.; Newman, M.; Sein, M.K. (2017): The public procurement of information systems: dialectics in requirements specification. In: European Journal of Information Systems, Vol. 26 (2017) No. 2, pp. 143-163.

Moores, T. (2005): Do consumers understand the role of privacy seals in e-commerce? In: Communications of the ACM, Vol. 48 (2005) No. 3, pp. 86-91.

Morgan, L.; Conboy, K. (2013): Factors affecting the adoption of cloud computing: an exploratory study. *Proceedings of the European Conference on Information Systems*. Utrecht.

Mousavizadeh, M.; Kim, D. (2015): A study of the effect of privacy assurance mechanisms on self-disclosure in social networking sites from the view of protection motivation theory. *International Conference on Information Systems* Fort Worth.

Müller-Bloch, C.; Kranz, J. (2015): A framework for rigorously identifying research gaps in qualitative literature reviews. *International Conference on Information Systems*. Fort Worth.

Myers, M.D. (1997): Qualitative research in information systems. In: Management Information Systems Quarterly, Vol. 21 (1997) No. 2, pp. 241-242.

Nag, S.N., Fred; Graham, Colleen; Biscotti, Fabrizio; Swinehart, Hai Hong (2017): Forecast Analysis: Public Cloud Services, Worldwide, 3Q17 Update. https://www.gartner.com/doc/3837566/forecast-analysis-public-cloud-services, accessed at

Nakata, C.; Sivakumar, K. (1996): National culture and new product development: An integrative review. In: Journal of Marketing, Vol. 60 (1996) No. 1, pp. 61-72.

Nakatsu, R.T.; Iacovou, C.L. (2009): A comparative study of important risk factors involved in offshore and domestic outsourcing of software development projects: A two-panel Delphi study. In: Information & Management, Vol. 46 (2009) No. 1, pp. 57-68.

Noordewier, T.G.; John, G.; Nevin, J.R. (1990): Performance outcomes of purchasing arrangements in industrial buyer-vendor relationships. In: Journal of Marketing, Vol. 54 (1990) No. 4, pp. 80-93.

Oezpolat, K.; Gao, G.; Jank, W.; Viswanathan, S. (2013): The value of third-party assurance seals in online retailing: An empirical investigation. In: Information Systems Research, Vol. 24 (2013) No. 4, pp. 1100-1111.

Okoli, C.; Pawlowski, S.D. (2004): The Delphi method as a research tool: an example, design considerations and applications. In: Information & Management, Vol. 42 (2004) No. 1, pp. 15-29.

Oliveira, T.; Thomas, M.; Espadanal, M. (2014): Assessing the determinants of cloud computing adoption: An analysis of the manufacturing and services sectors. In: Information & Management, Vol. 51 (2014) No. 5, pp. 497-510.

Orlikowski, W.J.; Baroudi, J.J. (1991): Studying information technology in organizations: Research approaches and assumptions. In: Information Systems Research, Vol. 2 (1991) No. 1, pp. 1-28.

Pagani, M. (2013): Digital business strategy and value creation: Framing the dynamic cycle of control points. In: Management Information Systems Quarterly, Vol. 37 (2013) No. 2, pp. 617-632.

Pare, G.; Cameron, A.-F.; Poba-Nzaou, P.; Templier, M. (2013): A systematic assessment of rigor in information systems ranking-type Delphi studies. In: Information & Management, Vol. 50 (2013) No. 5, pp. 207-217.

Pavlou, P.A. (2002): Institution-based trust in interorganizational exchange relationships: The role of online B2B marketplaces on trust formation. In: The Journal of Strategic Information Systems, Vol. 11 (2002) No. 3, pp. 215-243.

Pavlou, P.A. (2011): State of the information privacy literature: where are we now and where should we go? In: Management Information Systems Quarterly, Vol. 35 (2011) No. 4, pp. 977-988.

Pavlou, P.A.; Fygenson, M. (2006): Understanding and predicting electronic commerce adoption: An extension of the theory of planned behavior. In: Management Information Systems Quarterly, Vol. 30 (2006) No. 1, pp. 115-143.

Pavlou, P.A.; Liang, H.; Xue, Y. (2006): Understanding and mitigating uncertainty in online environments: A principal-agent perspective. In: Management Information Systems Quarterly, Vol. 31 (2006) No. 1, pp. 105-136.

Petri, I.; Diaz-Montes, J.; Zou, M.; Beach, T.; Rana, O.; Parashar, M. (2015): Market models for federated clouds. In: IEEE Transactions on Cloud Computing, Vol. 3 (2015) No. 3, pp. 398-410.

Petter, S.; Straub, D.; Rai, A. (2007): Specifying formative constructs in information systems research. In: Management Information Systems Quarterly, Vol. 31 (2007) No. 4, pp. 623-656.

Pflügler, C.; Wiesche, M.; Krcmar, H. (2015): Are we already in a mature ITO market? A longitudinal study on the effects of market maturity on ITO vendor project performance. *International Conference on Information Systems*. Fort Worth.

Pinsonneault, A.; Kraemer, K. (1993): Survey research methodology in management information systems: an assessment. In: Journal of management information systems, Vol. 10 (1993) No. 2, pp. 75-105.

Podsakoff, P.M.; MacKenzie, S.B.; Lee, J.-Y.; Podsakoff, N.P. (2003): Common method biases in behavioral research: a critical review of the literature and recommended remedies. In: Journal of Applied Psychology, Vol. 88 (2003) No. 5, pp. 879-903.

Polites, G.L.; Roberts, N.; Thatcher, J. (2012): Conceptualizing models using multidimensional constructs: a review and guidelines for their use. In: European Journal of Information Systems, Vol. 21 (2012) No. 1, pp. 22-48.

Poppo, L.; Zenger, T. (2002): Do formal contracts and relational governance function as substitutes or complements? In: Strategic Management Journal, Vol. 23 (2002) No. 8, pp. 707-725.

Purohit, D.; Srivastava, J. (2001): Effect of manufacturer reputation, retailer reputation, and product warranty on consumer judgments of product quality: A cue diagnosticity framework. In: Journal of Consumer Psychology, Vol. 10 (2001) No. 3, pp. 123-134.

Ragowsky, A.; Licker, P.; Miller, J.; Gefen, D.; Stern, M. (2014): Do Not Call Me Chief Information Officer, but Chief Integration Officer. A summary of the 2011 detroit CIO roundtable. In: Communications of the Association for Information Systems, Vol. 34 (2014) No. 1, pp. 1333-1346.

Rai, A.; Maruping, L.M.; Venkatesh, V. (2009): Offshore information systems project success: the role of social embeddedness and cultural characteristics. In: Management Information Systems Quarterly, Vol. 33 (2009) No. 3, pp. 617-641.

Ramacher, D.-I.R.; Mönch, L. (2014): Robust multi-criteria service composition in information systems. In: Business & Information Systems Engineering, Vol. 6 (2014) No. 3, pp. 141-151.

Ramgovind, S.; Eloff, M.M.; Smith, E. (2010): The management of security in cloud computing. *Information Security for South Africa* (pp. 1-7). Johannesburg: IEEE.

Ran, S. (2003): A model for web services discovery with QoS. In: ACM SIGecom Exchanges, Vol. 4 (2003) No. 1, pp. 1-10.

Remus, U.; Wiener, M.; Saunders, C.; Mähring, M.; Kofler, M. (2016): Control Modes Versus Control Styles: Investigating ISD Project Control Effects at the Individual Level. Paper presented at the International Conference on Information Systems, Dublin.

Repschlaeger, J.; Wind, S.; Zarnekow, R.; Turowski, K. (2013): Decision model for selecting a cloud provider: A study of service model decision priorities. *Americas Conference on Information Systems*. Chicago.

Repschlaeger, J.; Zarnekow, R.; Wind, S.; Turowski, K. (2012): Cloud Requirement Framework: Requirements and Evaluation Criteria to Adopt Cloud solutions. Paper presented at the Proceedings of the European Conference on Information Systems (ECIS) 2012, Barcelona, Spain, pp. 42.

Repschläger, J.; Wind, S.; Zarnekow, R.; Turowski, K. (2011): Developing a Cloud Provider Selection Model. Paper presented at the Enterprise Modelling and Information Systems Architectures, Hamburg, Germany, pp. 163-176.

Rieger, P.; Gewald, H.; Schumacher, B. (2013): Cloud-Computing in Banking Influential Factors, Benefits and Risks from a Decision Maker's Perspective. *Americas Conference on Information Systems*. Chicago.

Rindfleisch, A.; Heide, J.B. (1997): Transaction cost analysis: Past, present, and future applications. In: Journal of Marketing, Vol. 61 (1997) No. 4, pp. 30-54.

Rustagi, S.; King, W.R.; Kirsch, L.J. (2008): Predictors of formal control usage in IT outsourcing partnerships. In: Information Systems Research, Vol. 19 (2008) No. 2, pp. 126-143.

Saleem, M.S.; Ding, C.; Liu, X.; Chi, C.-H. (2015): Personalized decision-strategy based web service selection using a learning-to-rank algorithm. In: IEEE Transactions on Services Computing, Vol. 8 (2015) No. 5, pp. 727-739.

Salehan, M.; Kim, D.J.; Lee, J.-N. (2015): Antecedents, processes and consequences of web assurance seals: A meta-analysis approach. *Pacific Asia Conference on Information Systems*. Singapore.

Salipante, P.; Notz, W.; Bigelow, J. (1982): A matrix approach to literature reviews. In: Research in organizational behavior, Vol. 4 (1982), pp. 321-348.

Saripalli, P.; Pingali, G. (2011): Madmac: Multiple attribute decision methodology for adoption of clouds. *IEEE International Conference on Cloud Computing* (pp. 316-323). Washington.

Saya, S.; Pee, L.G.; Kankanhalli, A. (2010): The impact of institutional influences on perceived technological characteristics and real options in cloud computing adoption. *International Conference on Information Systems* (pp. 24). St. Louis.

Schermann, M.; Dongus, K.; Yetton, P.; Krcmar, H. (2016): The role of transaction cost economics in information technology outsourcing research: a meta-analysis of the choice of contract type. In: The Journal of Strategic Information Systems, Vol. 25 (2016) No. 1, pp. 32-48.

Schermann, M.; Wiesche, M.; Krcmar, H. (2012): The role of information systems in supporting exploitative and exploratory management control activities. In: Journal of Management Accounting Research, Vol. 24 (2012) No. 1, pp. 31-59.

Schmidt, R.; Lyytinen, K.; Mark Keil, P.C. (2001): Identifying software project risks: An international Delphi study. In: Journal of Management Information Systems, Vol. 17 (2001) No. 4, pp. 5-36.

Schmidt, R.C. (1997): Managing Delphi Surveys Using Nonparametric Statistical Techniques. In: Decision Sciences, Vol. 28 (1997) No. 3, pp. 763-774.

Schneider, S.; Sunyaev, A. (2016): Determinant factors of cloud-sourcing decisions: reflecting on the IT outsourcing literature in the era of cloud computing. In: Journal of Information Technology, Vol. 31 (2016) No. 1, pp. 1-31.

Schneider, S.; Wollersheim, J.; Krcmar, H.; Sunyaev, A. (2018): How do requirements evolve over time? A case study investigating the role of context and experiences in the evolution of enterprise software requirements. In: Journal of Information Technology, Vol. 33 (2018) No. 2, pp. 151-170.

Schreieck, M.; Wiesche, M.; Krcmar, H. (2016): Design and Governance of Platform Ecosystems-Key Concepts and Issues for Future Research. Paper presented at the European Conference on Information Systems, Istanbul, pp. ResearchPaper76.

Schrödl, H. (2012): Purchasing Cloud-Based Product-Service Bundles in Value Networks-the Role of Manageable Workloads. *European Conference on Information Systems*. Barcelona.

Schwartz, P.M. (2004): Property, privacy, and personal data. In: Harvard Law Review, Vol. 117 (2004) No. 7, pp. 2056-2128.

Schwarz, A.; Jayatilaka, B.; Hirschheim, R.; Goles, T. (2009): A conjoint approach to understanding IT application services outsourcing. In: Journal of the Association for Information Systems, Vol. 10 (2009) No. 10, pp. 748-781.

Sethi, V.; King, R.C. (1999): Nonlinear and noncompensatory models in user information satisfaction measurement. In: Information Systems Research, Vol. 10 (1999) No. 1, pp. 87-96.

Shaked, A.; Sutton, J. (1982): Imperfect information, perceived quality, and the formation of professional groups. In: Journal of Economic Theory, Vol. 27 (1982) No. 1, pp. 170-181.

Shapiro, D.L.; Sheppard, B.H.; Cheraskin, L. (1992): Business on a handshake. In: Negotiation Journal, Vol. 8 (1992) No. 4, pp. 365-377.

Sheeran, P. (2002): Intention - behavior relations: A conceptual and empirical review. In: European review of social psychology, Vol. 12 (2002) No. 1, pp. 1-36.

Simonin, B.L.; Ruth, J.A. (1998): Is a company known by the company it keeps? Assessing the spillover effects of brand alliances on consumer brand attitudes. In: Journal of Marketing Research, Vol. 35 (1998) No. 1, pp. 30-42.

Singh, R.; Keil, M.; Kasi, V. (2009): Identifying and overcoming the challenges of implementing a project management office. In: European Journal of Information Systems, Vol. 18 (2009) No. 5, pp. 409-427.

Siponen, M.; Vance, A. (2014): Guidelines for improving the contextual relevance of field surveys: the case of information security policy violations. In: European Journal of Information Systems, Vol. 23 (2014) No. 3, pp. 289-305.

Sitkin, S.B.; Pablo, A.L. (1992): Reconceptualizing the determinants of risk behavior. In: Academy of Management Review, Vol. 17 (1992) No. 1, pp. 9-38.

Skinner, E.A. (1996): A guide to constructs of control. In: Journal of Personality and Social Psychology, Vol. 71 (1996) No. 3, pp. 549-570.

Smith, H.J.; Dinev, T.; Xu, H. (2011): Information privacy research: an interdisciplinary review. In: Management Information Systems Quarterly, Vol. 35 (2011) No. 4, pp. 989-1016.

Smith, H.J.; Milberg, S.J.; Burke, S.J. (1996): Information privacy: measuring individuals' concerns about organizational practices. In: Management Information Systems Quarterly, Vol. 20 (1996) No. 2, pp. 167-196.

Smith, V.L. (1976): Experimental economics: Induced value theory. In: American Economic Review, Vol. 66 (1976) No. 2, pp. 274-279.

Söllner, M.; Hoffmann, A.; Leimeister, J.M. (2015): Why different trust relationships matter for information systems users. In: European Journal of Information Systems, Vol. 25 (2015) No. 33, pp. 274-287.

Son, J.-Y.; Benbasat, I. (2007): Organizational buyers' adoption and use of B2B electronic marketplaces: efficiency-and legitimacy-oriented perspectives. In: Journal of Management Information Systems, Vol. 24 (2007) No. 1, pp. 55-99.

Son, J.-Y.; Kim, S.S. (2008): Internet users' information privacy-protective responses: A taxonomy and a nomological model. In: Management Information Systems Quarterly, Vol. 32 (2008) No. 3, pp. 503-529.

Spears, J.L. (2013): The effects of notice versus awareness: An empirical examination of an online consumer's privacy risk treatment. *Hawaii International Conference on System Sciences* (pp. 3229-3238). Wailea: IEEE.

Spiekermann, S. (2005): Perceived control: Scales for privacy in ubiquitous computing. Paper presented at the International Conference on User Modeling, Edinburgh.

Srite, M.; Karahanna, E. (2006): The role of espoused national cultural values in technology acceptance. In: Management Information Systems Quarterly, Vol. 30 (2006) No. 3, pp. 679-704.

Srivastava, R.P.; Mock, T.J. (1999a): Evidential reasoning for WebTrust assurance services. *Hawaii International Conference on Systems Sciences* (Vol. Track5, pp. 10 pp.). Maui.

Srivastava, R.P.; Mock, T.J. (1999b): Evidential reasoning for WebTrust assurance services. In: Journal of Management Information Systems, Vol. 16 (1999b) No. 3, pp. 11-32.

Straub, D.; Boudreau, M.-C.; Gefen, D. (2004): Validation guidelines for IS positivist research. In: Communications of the Association for Information Systems, Vol. 13 (2004) No. 1, pp. 380-427.

Straub, D.W. (1989): Validating instruments in MIS research. In: Management Information Systems Quarterly, Vol. 13 (1989) No. 2, pp. 147-169.

Straub, D.W.; Gefen, D.; Boudreau, M.-C. (2005): Quantitative research (Vol. 1), Elsevier, Amsterdam 2005.

Strauss, A.L.; Corbin, J.M. (1990): Basics of qualitative research (Vol. 15), Sage Newbury Park, USA 1990.

Su, F.; Mao, J.-Y.; Jarvenpaa, S.L. (2014): How do IT outsourcing vendors respond to shocks in client demand? A resource dependence perspective. In: Journal of Information Technology, Vol. 29 (2014) No. 3, pp. 253-267.

Subashini, S.; Kavitha, V. (2011): A survey on security issues in service delivery models of cloud computing. In: Journal of Network and Computer Applications, Vol. 34 (2011) No. 1, pp. 1-11.

Sun, L.; Dong, H.; Hussain, F.K.; Hussain, O.K.; Chang, E. (2014): Cloud service selection: State-of-the-art and future research directions. In: Journal of Network and Computer Applications, Vol. 45 (2014), pp. 134-150.

Sun, L.; Srivastava, R.P.; Mock, T.J. (2006): An information systems security risk assessment model under the Dempster-Shafer theory of belief functions. In: Journal of Management Information Systems, Vol. 22 (2006) No. 4, pp. 109-142.

Sunyaev, A.; Schneider, S. (2013): Cloud services certification. In: Communications of the ACM, Vol. 56 (2013) No. 2, pp. 33-36.

Susarla, A.; Barua, A.; Whinston, A.B. (2003): Understanding the service component of application service provision: empirical analysis of satisfaction with ASP services. In: Management Information Systems Quarterly, Vol. 27 (2003) No. 1, pp. 91-123.

Sutton, S.G.; Khazanchi, D.; Hampton, C.; Arnold, V. (2008): Risk analysis in extended enterprise environments: Identification of critical risk factors in B2B e-commerce relationships. In: Journal of the Association for Information Systems, Vol. 9 (2008) No. 3-4, pp. 151-174.

Tang, Z.; Hu, Y.; Smith, M.D. (2008): Gaining trust through online privacy protection: Self-regulation, mandatory standards, or caveat emptor. In: Journal of Management Information Systems, Vol. 24 (2008) No. 4, pp. 153-173.

Terlaak, A.; King, A.A. (2006): The effect of certification with the ISO 9000 quality management standard: A signaling approach. In: Journal of Economic Behavior & Organization, Vol. 60 (2006) No. 4, pp. 579-602.

Tittle, C.R. (1980): Sanctions and social deviance: The question of deterrence, Praeger New York 1980.

Tiwana, A.; Bush, A.A. (2007): A comparison of transaction cost, agency, and knowledge-based predictors of IT outsourcing decisions: A US-Japan cross-cultural field study. In: Journal of Management Information Systems, Vol. 24 (2007) No. 1, pp. 259-300.

Tiwana, A.; Keil, M. (2009): Control in internal and outsourced software projects. In: Journal of Management Information Systems, Vol. 26 (2009) No. 3, pp. 9-44.

Tran, V.X.; Tsuji, H.; Masuda, R. (2009): A new QoS ontology and its QoS-based ranking algorithm for web services. In: Simulation Modelling Practice and Theory, Vol. 17 (2009) No. 8, pp. 1378-1398.

Truong-Huu, T.; Tham, C.-K. (2014): A novel model for competition and cooperation among cloud providers. In: IEEE Transactions on Cloud Computing, Vol. 2 (2014) No. 3, pp. 251-265.

Tschamler, H. (1996): Wissenschaftstheorie: Eine Einführung für Pädagogen (Vol. 3), Julius Klinkhardt, Bad Heilbrunn 1996.

Van der Valk, W.; Rozemeijer, F. (2009): Buying business services: towards a structured service purchasing process. In: Journal of Services Marketing, Vol. 23 (2009) No. 1, pp. 3-10.

Vance, A.; Elie-Dit-Cosaque, C.; Straub, D.W. (2008): Examining trust in information technology artifacts: the effects of system quality and culture. In: Journal of Management Information Systems, Vol. 24 (2008) No. 4, pp. 73-100.

Venkatesh, V.; Brown, S.A.; Bala, H. (2013): Bridging the qualitative-quantitative divide: Guidelines for conducting mixed methods research in information systems. In: Management Information Systems Quarterly, Vol. 37 (2013) No. 1, pp. 21-54.

Venkatesh, V.; Morris, M.G.; Davis, G.B.; Davis, F.D. (2003): User acceptance of information technology: Toward a unified view. In: Management Information Systems Quarterly, Vol. 27 (2003) No. 3, pp. 425-478.

Vom Brocke, J.; Simons, A.; Niehaves, B.; Riemer, K.; Plattfaut, R.; Cleven, A. (2009): Reconstructing the giant: On the importance of rigour in documenting the literature search process. *European Conference on Information Systems* (Vol. 9, pp. 2206-2217). Verona.

Wang, J.; Chaudhury, A.; Rao, H.R. (2008): Research note - A value-at-risk approach to information security investment. In: Information Systems Research, Vol. 19 (2008) No. 1, pp. 106-120.

Wang, P.; Du, X. (2016): QoS-aware service selection using an incentive mechanism. In: IEEE Transactions on Services Computing, (2016).

Wang, X.; Zhu, J.; Shen, Y. (2015): Network-aware QoS prediction for service composition using geolocation. In: IEEE Transactions on Services Computing, Vol. 8 (2015) No. 4, pp. 630-643.

Warren, S.D.; Brandeis, L.D. (1890): The right to privacy. In: Harvard Law Review, Vol. 4 (1890) No. 5, pp. 193-220.

Webster, J.; Watson, R.T. (2002): Analyzing the past to prepare for the future: Writing a literature review. In: Management Information Systems Quarterly, Vol. 26 (2002) No. 2, pp. xiii-xxiii.

Weinhardt, C.; Anandasivam, A.; Blau, B.; Borissov, N.; Meinl, T.; Michalk, W.; Stößer, J. (2009): Cloud computing – A classification, business models, and research directions. In: Business & Information Systems Engineering, Vol. 1 (2009) No. 5, pp. 391-399.

Weisz, J.R.; Rothbaum, F.M.; Blackburn, T.C. (1984): Standing out and standing in: The psychology of control in America and Japan. In: American Psychologist, Vol. 39 (1984) No. 9, pp. 955-969.

Westin, A.F. (1968): Privacy and freedom. In: Washington and Lee Law Review, Vol. 25 (1968) No. 1, pp. 166-170.

Westin, A.F. (2003): Social and political dimensions of privacy. In: Journal of Social Issues, Vol. 59 (2003) No. 2, pp. 431-453.

Whetten, D.A. (1989): What constitutes a theoretical contribution? In: Academy of Management Review, Vol. 14 (1989) No. 4, pp. 490-495.

Whiteside, F.; Badger, L.; Iorga, M.; Shilong, C. (2012): Challenging security requirements for US government cloud computing adoption. NIST, 2012.

Wiener, M.; Mähring, M.; Remus, U.; Saunders, C. (2016): Control Configuration and Control Enactment in Information Systems Projects: Review and Expanded Theoretical Framework. In: Management Information Systems Quarterly, Vol. 40 (2016) No. 3, pp. 741-774.

Wiesche, M.; Bodner, J.; Schermann, M. (2012): Antecedents of IT-enabled organizational control mechanisms. Paper presented at the European Conference on Information Systems, Barcelona.

Wiesche, M.; Jurisch, M.C.; Yetton, P.W.; Krcmar, H. (2017): Grounded theory methodology in information systems research. In: Management Information Systems Quarterly, Vol. 41 (2017) No. 3, pp. 685-701.

Wiesche, M.; Schermann, M.; Krcmar, H. (2015): Understanding the enabling design of IT risk management processes. *International Conference on Information Systems*. Fort Worth.

Williams, T. (1997): Interorganisational information systems: Issues affecting interorganisational cooperation. In: The Journal of Strategic Information Systems, Vol. 6 (1997) No. 3, pp. 231-250.

Wollersheim, J.; Krcmar, H. (2013): Purchasing processes for cloud services-An exploratory study of process influencing factors. *International Purchasing and Supply Education and Research Association Conference* (pp. 1285-1295). Nantes, France.

Woods, V. (2016): Gartner says worldwide public cloud services market is forecast to reach $204 billion in 2016. http://www.gartner.com/newsroom/id/3188817, accessed at Accessed on 2016-06-01.

Wright, R.T.; Campbell, D.E.; Thatcher, J.B.; Roberts, N. (2012): Operationalizing multidimensional constructs in structural equation modeling: Recommendations for IS research. In: Communications of the Association for Information Systems, Vol. 30 (2012) No. 1, pp. 367-412.

Wu, W.-W.; Lan, L.W.; Lee, Y.-T. (2011): Exploring decisive factors affecting an organization's SaaS adoption: A case study. In: International Journal of Information Management, Vol. 31 (2011) No. 6, pp. 556-563.

Xiao, B.; Benbasat, I. (2007): E-commerce product recommendation agents: Use, characteristics, and impact. In: Management Information Systems Quarterly, Vol. 31 (2007) No. 1, pp. 137-209.

Xin, M.; Levina, N. (2008): Software-as-a-service model: Elaborating client-side adoption factors. Paper presented at the Proceedings of the 29th International Conference on Information Systems (ICIS) 2008, Paris, France.

Xu, H.; Crossler, R.E.; BéLanger, F. (2012a): A value sensitive design investigation of privacy enhancing tools in web browsers. In: Decision Support Systems, Vol. 54 (2012a) No. 1, pp. 424-433.

Xu, H.; Dinev, T.; Smith, J.; Hart, P. (2011): Information privacy concerns: Linking individual perceptions with institutional privacy assurances. In: Journal of the Association for Information Systems, Vol. 12 (2011) No. 12, pp. 798-824.

Xu, H.; Teo, H.-H. (2004): Alleviating consumers' privacy concerns in location-based services: A psychological control perspective. *International Conference on Information Systems* (pp. 64). Charlottesville.

Xu, H.; Teo, H.-H.; Tan, B.C.; Agarwal, R. (2012b): Research note - Effects of individual self-protection, industry self-regulation, and government regulation on privacy concerns: a study of location-based services. In: Information Systems Research, Vol. 23 (2012b) No. 4, pp. 1342-1363.

Yamagishi, T.; Yamagishi, M. (1994): Trust and commitment in the United States and Japan. In: Motivation and Emotion, Vol. 18 (1994) No. 2, pp. 129-166.

Yamaguchi, S. (2001): Culture and control orientations, Oxford University Press, New York 2001.

Yan, A.; Solomon, S.; Mirchandani, D.; Lacity, M.; Porra, J. (2013): The role of service agent, service quality, and user satisfaction in self-service technology. *International Conference on Information Systems*. Milan.

Yan, J.K.; Wakefield, R. (2015): Cloud Storage Services: Converting the Free-Trial User to a Paid Subscriber. Paper presented at the International Conferences on Information Systems, Fort Worth.

Yang, H.; Tate, M. (2012): A descriptive literature review and classification of cloud computing research. In: Communications of the Association for Information Systems, Vol. 31 (2012) No. 2, pp. 35-60.

Yin, R.K. (2013): Case study research: Design and methods, Sage publications 2013.

Zhao, X.; Xue, L.; Whinston, A.B. (2009): Managing interdependent information security risks: A study of cyberinsurance, managed security service and risk pooling. Paper presented at the International Conference on Information Systems, Phoenix, pp. 49.

Zhou, J.; Niemela, E.; Savolainen, P. (2007): An integrated QoS-aware service development and management framework. *Working IEEE/IFIP Conference on Software Architecture* (pp. 13-13). Mumbai.

Appendix

Appendix A: Overview of assurance research

Citation	Relational Assurance Mechanism Examples [1]	Antecedent			Effect											
		Concern			Belief					Intention				Behavior		
		Privacy	Security	Business Integrity	Trust	Structural Assurance	Satisfaction	Concern	Risks	Information Disclosure	Purchase	Continuance	Usage	Information Disclosure	Purchase	Price Premium
(Akter et al. 2010)	SI	x	x			x	x						x			
(Aubert et al. 2012)	Stand							x								
(Ba/Pavlou 2002)	FM; Rep				x											x
(Bansal/Zahedi 2008)	Stat; SQ; Cert; CN; Rep	x			x					x						
(Bansal et al. 2015)	Stat; SQ; Cert; CN; Rep; Rec	x			x					x						
(Chandra et al. 2010)		x	x			x							x			
(Chen/Chien 2009)		x	x		x	x							x			
(Chen/Mitchell 2010)	SI	x	x	x		x		x								
(Devaraj et al. 2002)			x			x	x									
(Dimoka et al. 2012)	PD; Cert; FM; W			x				x								x
(Gundlach/Cannon 2010)	M															
(Huang et al. 2005)	Rep; SQ	x	x		x	x			x	x	x					
(Hui et al. 2007)	Stat; Cert	x						x						x		
(Johnston/Warkentin 2010)	Rec; Pers; SI		x													
(Keith et al. 2010)	Cert; Rec; SQ; SI	x							x		x		x			
(Keith et al. 2011)	Cert; SQ	x			x						x		x			
(Keith et al. 2015)	Cert; Rec; SQ; Pers; FM; Stat; SI	x	x		x	x								x		
(Khazanchi/Sutton 2001)	Cert	x	x	x												
(Kim/Benbasat 2006)	Stat	x	x		x											
(Kim/Benbasat 2009)	Stat	x	x		x											
(Kim et al. 2015)	Cert; W	x	x	x							x					
(Kimery/McCord 2002b)	Cert	x	x	x												
(Kim/Koohikamali 2015)	Stat	x														
(Krasnova/Veltri 2010)	L	x												x		
(Kuan/Bock 2005)	FM; Rep				x	x					x					
(Liao 2005)	SQ; Rep	x	x		x	x										
(Li et al. 2013)	Cert; FM; PD; W	x	x								x					
(Lowry et al. 2015)		x	x		x											
(Lowry et al. 2008)	SQ; Rep	x	x		x											
(Mäntymäki 2008)		x	x		x	x										
(McKnight et al. 2002a)	SQ; Rep	x	x		x	x			x	x	x					
(McKnight et al. 2002b)	SQ; Rep	x	x		x	x				x	x					
(Mousavizadeh/Kim 2015)	Stat; Pers	x				x		x	x					x		

(Oezpolat et al. 2013)	Cert	x	x	x										x
(Pavlou 2002)	M; FM; CN		x				x		x	x	x			
(Pavlou et al. 2006)	PD; SQ; Rep; W; SI	x	x	x				x		x				x
(Salehan et al. 2015)	Cert	x	x	x	x	x			x	x			x	
(Son/Kim 2008)		x												
(Spears 2013)		x							x			x		
(Srivastava/Mock 1999a)	Cert		x	x										
(Srivastava/Mock 1999b)	Cert		x	x										
(Sun et al. 2006)	Cert		x											
(Sutton et al. 2008)	Cert	x	x	x										
(Wang et al. 2008)	Red		x											
(Xu et al. 2011)	Stat; Cert	x						x	x					
(Xu/Teo 2004)	Stat; Cert; L; Pers; Rep	x						x				x		
(Xu et al. 2012b)	Stat; Cert; L; Pers; Rep	x						x						
(Yan et al. 2013)	SI		x			x	x							

[1] Cert = Certification, CN = Corporative norm, FM = Feedback mechanism, L = Law, M = Monitoring, Pers = Personalization, PD = Product description, Red = Redundancy, Rec = Recommendation, Rep = Reputation, SQ = Site quality, SI = Social Influence, Stand = Standardization, Stat = Statement, W = Warranty

Table 3. Overview of Assurance Research

Appendix B: QoS attribute identification process

At the beginning of the one-to-one brainstorming, the researcher explained the research target, motivated the participant to state as many QoS attributes as possible, and restrained from judging or evaluating any responses (Gallupe et al. 1991). Subsequently, the researcher conducted a semi-structured interview with each participant. On the basis of our research target, the semi-structured interview guide included questions to identify technical QoS attributes, operation-related aspects, and managerial QoS attributes to help participants reach a certain level of confidence during CSP selection decisions. Questions related to technical QoS included "Which operational requirements must or should a cloud service provider meet?". Questions related to managerial QoS attributes included "What information during your selection decision helps you to select the right CSP?". The research included some of the mentioned QoS from the brainstorming within the semi-structured interview to collect background information. After each interview, the authors discussed the results and iteratively adjusted the semi-structured interview guide.

Figure 20 illustrates an overview of the QoS attribute identification process.

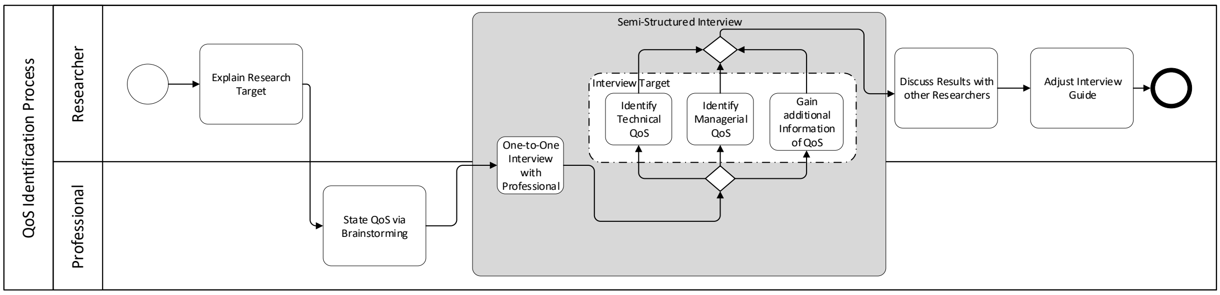

QoS Identification Process
Researcher
Professional
Explain Research Target
State QoS via Brainstorming
One-to-One Interview with Professional
Semi-Structured Interview
Interview Target
Identify Technical QoS
Identify Managerial QoS
Gain additional Information of QoS
Discuss Results with other Researchers
Adjust Interview Guide

Figure 20. QoS attribute identification process

Appendix C: Selected codes from QoS coding process

As an example of our coding process, Table 45 outlines selected codes and selected derived QoS attributes.

Selected code (total 69)	QoS attribute (total 31)
certificate renewal reporting	Certification
certification authority	
penalties in contract	Contract
service level agreements	
network security specification	Functionality
performance	
geolocation of servers	Geolocation of servers
home market provider	
dashboard of service level agreement	Monitoring
data modification report	
providers’ service hotline	Support
providers support	
free system releases	Test of solution
test of solution	
sub-providers clarity	Transparency of activities
transparency of failure handling	

Table 45. Examples of codes and derived QoS attributes for cloud service provider selection

Appendix D: QoS attribute description process

Members of our professional panel had different job positions and were from different industries, it was fundamental to assure that each panel member had the same understanding of each single QoS attribute. On the basis of the interviews, the researchers provided an initial description of each QoS. Participants were then asked to comment on the description using two options: the participant either had minor issues with the description and could provide possible extensions or minor changes, or the participant had major issues and disagreed with the provided description or had fundamental change requirements. In the case of major issues, the researchers discussed the change requirement during a follow-up telephone interview and, if required, adjusted the description accordingly. For example, major issues arose for legal compliance and geolocation of servers. Initially, geolocation of servers and legal compliance were used as synonyms. Following discussion, the researchers decided to split these constructs according to the opinions of the participants. After the changes were introduced, the participants were asked to make any further corrections and again validate the resulting descriptions. After two iterations, the participants agreed on the provided QoS descriptions.

Figure 21 illustrates an overview on the QoS attribute description process.

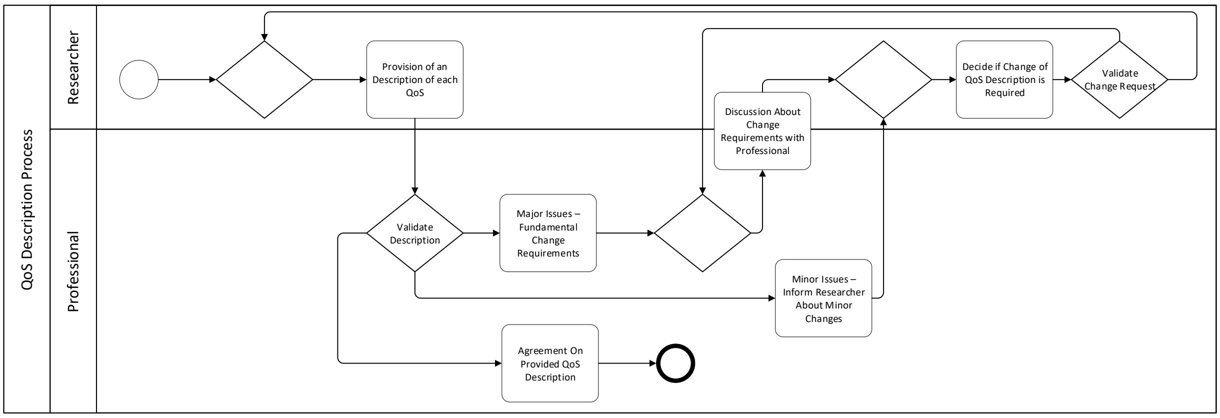

QoS Description Process
Researcher
Professional
Provision of an Description of each QoS
Discussion About Change Requirements with Professional
Decide if Change of QoS Description is Required
Validate Change Request
Validate Description
Major Issues – Fundamental Change Requirements
Minor Issues – Inform Researcher About Minor Changes
Agreement On Provided QoS Description

Figure 21. QoS attribute description process

Appendix E: Selected quotes from our professional panelists

Cloud customers use *certificates* during the CSP selection process to assure data protection. Certificates inform the cloud customer that an authority conducted an audit to verify that the CSP is compliant with a range of certification criteria. Cloud customers use certificates to have a standardized tool to compare the capabilities of the CSP. One of our professionals illustrates the value of certificates during CSP selection:

> "*Certificates can help to directly compare different CSP. Based on certificates I can say 'ok, this cloud solution is certified for data security to 95% and this is 99% data-secured.' Then my decision would probably always be to go with the higher certificate."* (Business Intelligence Manager #2)

Cloud customers may have limited knowledge about verification of the capabilities of CSP. Cloud customers outsource their information systems and buy services on-demand from the CSP, which may mean that knowledge and capabilities are no longer within the cloud customers' company (Schneider/Sunyaev 2016). To assure compliance with existing laws and protect data, certification authorities support cloud customers during CSP selection by providing a certification attestation. One of our professionals described the value of certificates during CSP selection as follows:

> "We do not have the resources to investigate the infrastructure and processes of possible CSP by ourselves. We rely on judgements of auditors who frequently conduct cloud audits. Those guys are well experienced and even more capable than we are in regard to evaluating the CSP*." (*IT-Manager #14*)*

Information on the *geolocation of servers* is valuable for the cloud customer. Regional laws in place affect the level of compliance CSP reaches. While the European zone established a high level of data protection laws (for example, with regard to China), data protection laws are limited (Dove et al. 2015). Cloud customers use such information to indirectly assure data protection and select CSP according to their own requirements. As noted by a professional, the knowledge of the geolocation of servers is a pre-condition to consider a CSP during the selection process.

> *"Personally for me I would prefer the servers not to be in China or in Russia and I can probably guarantee 100% that none of [CSP 1]s', [CSP2]s', or [CSP3]s' servers are in those countries. And if this is a less-known company and a less-known provider, the geolocation of servers would be even more important during my selection decision." (*Consultant Manager #6*)*

A *cloud exit strategy* articulates clear steps, which are required to run through when and if a business customer decides to exit the cloud service in future. A cloud service strategy can become obsolete overnight due to changes in business strategy (Rai et al. 2009). To remain flexible, cloud customers require a cloud exit strategy to export data to their own IT landscape or migrate data from one cloud service to another after changes in their business strategy occur:

> *"I want to know in advance if and exactly how a certain CSP is capable to perform an export from their service landscape. Unfortunately, from what I have seen and heard in many cases there is actually no exit strategy. Even the migration from one service to another having the same provider requires sometimes a lot of effort."* (Senior Consultant #8)

Test of solution refers to the possibility to use a free trial version of the cloud service. A variety of possible CSPs and offered services exist. At the same time, cloud customers have individual information systems in place and employees with different skills and competencies. To assure the possible cloud service fits to existing information systems and the targeted employee is capable of using these systems, cloud customers may try out a trial version of available services.

> *"I am also experimenting now with [the Cloud Service] from [CSP] and I am looking to test if it is potentially interesting and comfortable."* (Consultant Manager #6)

Appendix F: 31 unranked QoS attributes

QoS attribute	Description provided by professional panel
Assurance statement	Self-provided assurance statements of a CSP to address trust-related issues.
Benchmark	A CSP has high scores in an unbiased comparison of IT performance relative to peer organizations and those considered best-in-class.
Business process transparency	Transparency of CSP's organization structure, internal processes, roadmap, and development objectives.
Certification	A CSP is certified by an independent authority in accordance with established requirements or standards.
Cloud exit strategy	A CSP articulates clear cloud exit steps, which will take place when and if a business customer decides to exit its cloud in the future.
Contract	The provider offers understandable contractual arrangements including a clear cost structure (e.g., consumption-based pricing model).
Control	A CSP provides remote access tools to provide proactive control of data, functionalities, and processes (e.g., customization).
Deployment model	A clearly defined deployment model in terms of ownership, control of architectural design, and degree of available customization (e.g., private cloud, hybrid cloud, community cloud, and public cloud).
External business communication	Information about a CSP, its vision, services, and pricing is communicated clearly on provider's website, info sheets, etc.
Failure preventive measures	A CSP communicates unsuccessful preventive measures and mechanisms.
Financial performance	A CSP performs well financially, in terms of profit, revenue, equity, etc.
Flexibility	A customer can independently adjust the obtained capabilities, and the adjustments are carried out automatically within a short period of time and with transparent costs.
Functionality	The set of functions or capabilities (performance, availability, security, and scalability requirements) associated with the cloud solution matches the demands of the customer.
Geolocation of servers	Geographical location of providers' servers is suitable in terms of data protection legislation and user latency.
In-house recommendation	A CSP is highly recommended by a colleague, an IT-department member, or similar within a company.
Integration	Configuration of the service enables its smooth integration into the IT landscape of the business.
Interoperability	A customer can save and export data in standard formats, the cloud service offers open interfaces for integration with other cloud services or applications, and customers can access the cloud service location independently through various devices.
Legal compliance	Because of its geographical location, policies, etc., a CSP complies with legal and regulatory requirements of the customer.
Market share	The actual market share of a CSP.
Monitoring	A manual or automated IT monitoring and management technique, which provides transparency of cloud service quality.
Open communication	A CSP openly communicates previous incidents, failures, and their handling and predefines channels to report straightforwardly such situations if they occur in the future.
Ownership	Evident ownership of service hardware, software, etc. (by a CSP, a sub-provider, or others)
Personal contact	A CSP provides and establishes a strong personal contact.
Process maturity	The maturity of the business processes of the provider align with established best practices in the IT service sector.
Reputation	A CSP has earned a strong reputation in industry over time, confirmed by customer's portfolio, and evident in media, internet, or other information resources.
Standard operating environment	Consistency across operations enabling an easier cloud exit if necessary.

Support	A CSP possesses a responsive service support, which provides all operative processes necessary for the handling of service interruptions and for implementation of changes.
Test of solution	A CSP enables convenient trial periods of a service.
Third party recommendation	A CSP is highly recommended by a third party.
Track record	A CSP has a track record free of vulnerability incidents (such as data loss, data leakage, or hardware failure) widely known through media.
Transparency of activities	Transparency of security, data privacy, data access, cloud architecture, service level competencies, etc.

Table 46. Description of the 31 unranked QoS attributes for cloud service provider selection