

**MANAGEMENT OF RISKS DURING MIGRATION TO CLOUD COMPUTING: A
CASE STUDY**

by

Nathan Kilgore

SHARON GAGNON, PhD, Faculty Mentor and Chair

ALFREDO DOMINGUEZ, PhD, Committee Member

MILTON KABIA, PhD, Committee Member

Todd C. Wilson, PhD, Dean

School of Business and Technology

A Dissertation Presented in Partial Fulfillment

Of the Requirements for the Degree

Doctor of Information Technology

Capella University

July 2020

ProQuest Number:28094745

All rights reserved

INFORMATION TO ALL USERS

The quality of this reproduction is dependent on the quality of the copy submitted.

In the unlikely event that the author did not send a complete manuscript and there are missing pages, these will be noted. Also, if material had to be removed, a note will indicate the deletion.



ProQuest 28094745

Published by ProQuest LLC (2020). Copyright of the Dissertation is held by the Author.

All Rights Reserved.

This work is protected against unauthorized copying under Title 17, United States Code
Microform Edition © ProQuest LLC.

ProQuest LLC
789 East Eisenhower Parkway
P.O. Box 1346
Ann Arbor, MI 48106 - 1346

© Nathan Kilgore, 2020

Abstract

Businesses in the United States have been migrating to cloud computing for over a decade. There is no slowing in this movement. On the contrary, the proliferation of cloud computing migrations is happening at a faster pace than ever. There are numerous reasons these organizations are moving to the cloud, including popularity, cost, scalability, only paying for the resources used. There are many stumbling blocks to achieving a successful migration to the cloud. The research topic for this study was risk management in cloud migrations and how businesses work through the risks when they migrate to cloud computing. The methodology consisted of a case study of businesses that had migrated to cloud computing. The composition of the population of this research consisted of medium to large enterprise businesses in the United States that had migrated to cloud computing. Interviews with senior management, IT management, and IT practitioners from 3 different businesses in different industries were conducted. The interview questions were explicitly created by the study author to answer the question of how businesses operate and manage risks during cloud migration. Analysis of the research findings included NVivo and a process created by the study author using Microsoft Excel to process the research data. Analysis of the results provided coding for the themes found. Keywords and sentiment delivered themes that became the foundations of the data results. The findings of this research suggested that a light-weight framework could improve agility and provide businesses the ability to migrate to cloud computing without hindering the business. The reduction of effort and resources a business uses to migrate to cloud computing is directly associated with the preparation for risk evaluation and mitigation. A recommendation for future research to provide insight into risk mitigation of cloud migration regarding post cloud migration is noted. The use of this study provides the opportunity for existing IT professionals

to observe real world examples of cloud migration risk management in preparation for future cloud migrations.

Dedication

I dedicate this work to my family, Tonya, Wyatt, and Addyson. They have had to tolerate the many hours that I have spent away from them, and the missed basketball and volleyball games I did not witness, and the vacations I chose not to go on so I could complete my assignments along with this dissertation. They have supported, loved, and encouraged me to continue the quest to achieve this accomplishment. It is with the greatest admiration for my family that I dedicate this work to them.

Acknowledgments

I would like to acknowledge my committee chair, Dr. Sharon Gagnon, who guided me through the components of the dissertation process. I would further like to recognize my committee members, Dr. Alfredo Dominguez and Dr. Milton Kabia. My committee members further helped in streamlining this process in the completion of the Doctor of Information Technology. Lastly, I acknowledge and thank my cohort, the “Minions,” without whom I would not have completed this journey and accomplished this prodigious achievement.

Table of Contents

Acknowledgments	iv
List of Tables	vii
List of Figures	viii
CHAPTER 1. INTRODUCTION	1
Introduction	1
Background	2
Business Technical Problem	4
Research Purpose	5
Research Questions	6
Rationale	6
Theoretical Framework	7
Significance	9
Definition of Terms	10
Assumptions and Limitations	12
Organization for Remainder of Study	16
CHAPTER 2. LITERATURE REVIEW	17
Introduction	17
Review of the Literature	18
Conceptual Foundation for the Study	42
Conclusions	46
CHAPTER 3. METHODOLOGY	48
Introduction	48

Design and Methodology	48
Participants and Setting.....	50
Analysis of the Research Questions	55
Ethical Considerations	69
CHAPTER 4. RESULTS	73
Introduction.....	73
Data Collection Results.....	74
Data Analysis and Results	81
Summary	93
CHAPTER 5. CONCLUSIONS	95
Introduction.....	95
Evaluation of Research Questions	95
Fulfillment of Research Purpose.....	100
Contribution to Business Problem	101
Recommendations for Further Research.....	103
Conclusion	103
REFERENCES	105
APPENDIX.....	119

List of Tables

Table 1. Cloud Migration Data Collection Example	69
Table 2. Participant Demographics Detail	78
Table 3. Cloud Migration Detail	83
Table 4. Cloud Platform Type.....	84
Table 5. Risk Meeting Detail	88
Table 6. Risk Management Process Details	90
Table 7. Risk Management Responsibilities	91
Table 8. List of Risks by Type	98
Table 9. Risks that Became Issues	99

List of Figures

Figure 1. Change management method	38
Figure 2. Decision theory.....	39
Figure 3. Risk management cycle construct	40
Figure 4. Data collection flow chart.....	62

CHAPTER 1. INTRODUCTION

Introduction

Chapter 1 is organized into ten sections from the introduction through the summary. The ten sections provide the purpose, rationale, benefit, significance, limitations, and assumptions of this study. Additional sections provide the framework applied to this study and an explanation of this study topic. Further included are definitions of ambiguous terms, and technical acronyms used for the rest of this study. The last section of the first chapter contains the organization and structure of the full study.

Business firms in the United States are adopting cloud computing as the next iteration in technology (Bartoletti et al., 2017). Cloud migration by business firms in the United States is increasing (Kushida, Murray, & Zysman, 2015). The U.S. Department of Labor, Bureau of Labor Statistics (BLS, 2018) stated cloud computing as one of the key drivers for increased demand in IT occupations with the fastest growth rate of 13% between 2016 and 2026. Cloud computing will become the standard for business firms, with estimates suggesting over half a trillion dollars in spending on cloud computing within the next three years (Attaran, 2017).

Business firms in the United States in their haste to take advantage of cloud computing are not applying governance to cloud computing as they do to their on-premise infrastructure (Adjei, 2015). As an example, there exist two scenarios where the business either trusts the cloud vendor or the adoption of a cloud environment does not allow for governance to function the same as on-premise infrastructure (Information Systems Audit and Control Association

[ISACA], 2014). Both scenarios provide a risk for business firms. These scenarios are two of many causing risks associated with cloud migrations.

These moves from self-managed IT to vendor-managed infrastructure introduce risks that are threats to the business (Kosalge, 2015). A lack of knowledge of cloud computing provides the most significant risk to business firms adopting cloud computing (Alkhalil, Sahandi, & John, 2017). Federated computing is described as technology domains existing between both an on-premise and a partner location where trust exists between the two are becoming common (Dechouniotis, Dimolitsas, Papadakis-Vlachopapadopoulos, & Papavassiliou, 2018; Gartner, 2018). Business firms are not providing proper oversight and due diligence in planning for migration to a federated cloud computing environment (Islam, Fenz, Weippl, & Mouratidis, 2017).

Business firms in the United States are facing risks encountered as they migrate to cloud computing. Identification of the risks business firms encounter while adapting their technology base to cloud computing and remediation strategies, and plans are an ongoing issue (Nicho & Muumaar, 2016). Many risks exist that businesses encounter when adopting cloud computing (Islam et al., 2017). Well-known risks include security, availability, access, and compliance (Farah, 2015). The incidence of cloud computing migration in business firms in the United States was prevalent and topical at the time of this study (Bartoletti et al., 2017). Little literature exists describing the processes for managing risks encountered in real world scenarios by business firms migrating to cloud computing.

Background

Organizations are expanding into cloud computing business and technology models for reasons of performance, availability, and scalability all to create a competitive advantage

(Battleson, West, Kim, Ramesh, & Robinson, 2016). The demand to move to cloud computing is high for a majority of industries, and the growth of cloud migration is increasing across most industries (Bartoletti et al., 2017). The desire for business firms in the United States to adopt cloud computing is significant (Doherty, Carcary, & Conway, 2015). Cloud service providers attest business firms can adopt cloud computing without considering individual business needs and goals (ISACA, 2014).

Cloud service providers are promoting the benefits of cloud migration (Jede & Teuteberg, 2016). Business firms are compelling their IT departments to cloud migration without consideration of alignment with business goals to their detriment (Rahman, Islam, Kalloniatis, & Gritzalis, 2017). This urgency to adopt the next technology wave is also altering the way business firms' IT departments function (Farah, 2015). Disregard for basic governance practices exists due to the rush to adopt cloud computing by business firms in the United States (Islam et al., 2017). Business firms attempting to capitalize on the advantages of cloud migration must utilize forethought, planning, and implantation to reduce and prevent risks from materializing into issues that lead to adverse outcomes for the business firm (Gutierrez, Boukrami, & Lumsden, 2015; ISACA, 2014; Thomas, 2017).

The magnitude of the paradigm shift to cloud computing combined with the burden of monetary losses provides the need for a study of this phenomenon from a practical as well as academic point of view (Cărutasu & Cărutasu, 2016). There exists a gap in the literature regarding the risks business firms encounter during the migration to cloud computing (Priyadarshinee, Raut, Jha, & Gardas, 2017; Schneider & Sunyaev, 2016). The nascent amount of literature on such a prevalent landscape as cloud migration requires research into the phenomenon. The combination of the significant phenomenon of cloud migration and risk

management with a lack of studies provides significant interest to the researcher as a practitioner of cloud migrations.

Gartner (2016) asserted that businesses that do not plan for cloud migration are at risk of failure. A search of the literature does not produce existing information on how businesses manage risks that accompany migration during cloud computing (Schneider & Sunyaev, 2016). The construction of a conceptual framework for this study included decision theory and risk management theory. The themes were categorized and codified using the conceptual theory, an adaptation of the theory of design (Simon, 1996). Each participant brings their own experience and bias into any process (Slovic, 2016). This study reduces bias to the extent possible, providing the further granularity of each managed risk and the process involved from each participant's perspective. Each participant's role within the business aligns with their potential bias of the data collected (Slovic, 2016).

Business Technical Problem

Many firms have challenges managing the risks of cloud computing migration. Many businesses are migrating to the cloud. "Research and Markets" (2020) asserted that Microsoft had seen a grossly significant increase in cloud service use for 2020 in part due to the epidemic. Evidence provided by "Research and Markets" (2020) further suggests that medium and small businesses will be migrating to cloud offerings by 2025 in substantial numbers. "Research and Markets" (2020) emphasized that cloud migrations will continue through 2025, with over 85% of enterprises in the cloud the increase is observed in small and medium sized businesses migrating to the cloud. However, many businesses are failing in their attempt at cloud migration. Khalil (2019) suggested that there is an ongoing failure rate as high as 57% in late 2019. Cloud migration involves a great deal of risk (Fahmideh & Beydoun, 2017).

To address risk management difficulties, researchers focused on developing frameworks. Frameworks provide governance for applications, providers, operations, and services (Gartner, 2016). Frameworks create boundaries for businesses to align current practices with the shift to cloud computing (Fahmideh & Beydoun, 2017). Additional frameworks exist that businesses use to provide decisions regarding cloud migration risks (Islam et al., 2017). Despite this growing body of knowledge on risk management, the amount known about risk management processes in cloud migrations by business firms in the real world remains small.

Research Purpose

The purpose of this qualitative case study was to describe how business firms manage risks that they encounter during the migration of cloud computing. The population for this study was business firms in the United States, considered medium to large enterprises. The case subject for this study was large business firms in the United States. The business firms consisted of businesses that use enterprise software in the cloud. Each business firm had over 400 employees and annual revenue greater than 100 million dollars. The participants from each business included managers from the IT and business as well as IT practitioners. These managers and practitioners have direct knowledge and experience of the cloud migration of their business.

The findings of this study may be helpful for managers in planning for migrations to cloud computing. This study presents processes for risk management that managers benefit from by observing and learning from real world cases. This benefit for IT managers is helpful and provides the opportunity for managers to learn from real world examples and to avoid million-dollar mistakes (Cărutasu & Cărutasu, 2016; Vision Solutions, 2017). Managers can utilize the findings of this study to create a structure to begin planning for cloud migration risks.

Researchers have studied cloud migration and risks, as well as the risks associated with cloud migration. Other researchers have focused on frameworks for decision making on risks of cloud migration. Current knowledge about the risk management process of businesses during the cloud migration process is undeveloped. This study focused on real world examples of how business firms managed risks encountered during cloud migration.

Research Questions

The research question of this study was: How do enterprise businesses in the United States manage the risks that they encounter during the migration of cloud computing?

Rationale

Debreceeny (2013) stated a vibrant necessity for research of businesses where governance might play a decisive role in their vigilance towards realizing positive outcomes, thereby adding to the existing body of knowledge in information technology. Research is needed when IT resources have exceeded capacity, and the administration of those IT resources is so overwhelming the business chooses to migrate to cloud solutions without appreciating the complexity involved (Kauffman, Ma, & Yu, 2016; Rahman et al., 2017; Ray, 2016). Cărutasu and Cărutasu (2016) stated a large number of business firms are migrating to cloud computing, and as many businesses fail to achieve their goals of cloud migration. Islam et al. (2017) asserted a benefit to the creation and identification of such challenges as well as the creation of taxonomy to enable better measurement in the future.

Identification of the process used to manage risks by used real world business firms migrating to cloud computing is missing (Von Solms & Willett, 2017). This study presents findings that business firms can use to learn about identified risks and the processes used to manage them in real world scenarios. Chapter 4 presents the findings of this study, which

affords both practitioners and academics the ability to recognize lessons learned from the management of risks during cloud migration. This level of information enables businesses to mitigate deficiencies earlier in the cloud migration process. This study presents findings that organizations can use as a tool to provide an efficient allocation of resources.

Theoretical Framework

The underpinning of this conceptual framework was decision theory. Simon (1955, 1996) created decision theory based on human choice and their thinking processes. The first tenet of decision theory is guidance in what way to create the best decisions (Simon, 1955, 1996). The creation of the conceptual framework for this study used concepts adapted from Simon's decision theory.

This framework contains multiple concepts derived from Simon's decision theory, including definition, research, ideation, prototype, implementation, and evaluation (Simon, 1996). Other stages, as well as sub-concepts of decision theory, exist. Decision theory provides a framework that businesses can use in their risk management processes. Identification of the risk followed by the management process provides continuity of risk management. Following a standard risk management process improves the success of migrations to cloud computing (Islam et al., 2017). The key concepts of decision theory provide the best categorical and thematic markers for this study.

Simon (1955, 1996) defined a theory that described the ways managers make choices. Decision theory enables decision-making through key concepts. Decision management consists of six concepts:

- Define the problem.
- Research into the problem.

- Ideate possible solutions.
- Model solution.
- Implement solution.
- Evaluate the solution.

The next section defines the six steps of decision management. Characterizing the problem ensures an understanding of the scope of the issue involved. Research on the problem provides historical as well as up to date information. The use of this research is for brainstorming and other ways to solve this issue. Ideation is free-flow without constraints towards the creation of a single idea or many ideas to resolve the issue. The model solution brings ideas from a theoretical state to a practice state. Implementation applies the chosen model to provide a positive outcome to the issue. An evaluation provides a lessons-learned approach to understand if the implementation of the solution worked. This study was about the choices made by management during cloud migration. Specifically, the processes used to manage the risks encountered during cloud migration.

Decision theory includes details on the factors actors use to make business decisions (Simon, 1997). The decision theory was applicable in this study because the theory provides a theoretical lens in which may identify the emerging themes in how business firms manage risks that they encounter during migration to cloud computing. Businesses using the tenets of decision theory make better assessments when applied to the management of risks (Simon, 1996). The concepts of decision theory are employed to create categories for the sorting and coding of emerging themes for this study.

Significance

The findings of this study may be helpful for managers in planning for migrations to cloud computing. How large business firms manage risks they encounter during migration to the cloud is significant. Bartoletti et al. (2017) asserted that cloud migrations are increasing at a more significant rate year over year. Islam et al. (2017) indicated the necessity to identify significant risks in cloud computing migrations. Other researchers have focused on methods and frameworks of risks in cloud migration.

Practitioners will find the benefits of this study useful in cloud migrations. A large number of cloud migration failures each year is compelling businesses to look for external resources (Cărutasu & Cărutasu, 2016; Vision Solutions, 2017). The findings of this study could help other businesses. This study can provide a reference to IT managers as well as project and risk managers for businesses moving to cloud computing. The findings of this study contain known risks encountered through previous migrations as well as the processes used to manage them. Managers can add the risks presented as the findings of this study to their risk registers where appropriate.

In theory, the academic benefits of this study are in the research discovery. Researchers have predominately provided tools in the form of frameworks and methods for practitioners. This study provides a rich description using real world examples of businesses that have migrated to cloud computing. Cloud migration frameworks can be measured and validated against the outcome of this research. Each decision made by a business provides a gauge for academic evaluation through the evolution of cloud migrations. Business control and governance practices can use category frameworks for managing and processing risks of cloud migration.

Definition of Terms

Bureau of Labor and Statistics (BLS). The Department of Labor of the United States includes the BLS, which “measures labor market activity, working conditions, price changes, and productivity in the U.S. economy to support public and private decision making.” (BLS, 2018 para. 1)

Change management. Within the context of this study, change management refers to the Kurt Lewin model. Lewin asserted change management had three stages unfreeze, change, and freeze (Sarayreh, Khudair, & Barakat, 2013). By unfreezing the organization, the business could insert new, modify existing, or remove processes (Sarayreh et al., 2013). The change stage was the actual actionable stage adding, modifying, or removing processes (Sarayreh et al., 2013). The third and final stage was to put the business back in the state of being frozen to prevent changes without the consent of the business (Sarayreh et al., 2013).

Cloud computing. Cloud computing or the cloud has become ubiquitous with any form of technology service hosted by a third-party on the internet. Gartner (2018) defined cloud computing as a method of computing where technology capabilities deliver a scalable and dynamic service-oriented scheme to customers through the internet.

Common technologies. Technology, as referred to in this study, is used to indicate general or generic industry software, services, or delivery mechanisms related to computer infrastructure, which is used by most businesses within the United States.

Federated cloud infrastructure. Federated infrastructure identified through this study includes a combination of on-premise and subscribed services from a third-party provider that allows a business to utilize those services as a direct extension of the business’s self-controlled technology infrastructure.

High risk. A severe or catastrophic adverse effect where severe degradation in or a complete failure for the business to complete mission-critical operations to an extent and duration the business is not able to perform its primary functions, with significant damage to organizational assets; and or significant financial loss (NIST, 2004).

Information technology governance (ITG). ITG is the rules, process, procedures, and constructs used every day both in formal and informal practices by technology groups of organizations. Gartner (2018) defined ITG as the practices that safeguard the efficient and operational use of IT in empowering business to attain its objectives.

Infrastructure as a service (IaaS). IaaS enables the business to grow and scale-out without having a significant outlay of cost upfront to maximize business requirements. Gartner (2018) defined IaaS as a standardized, extreme automated subscription, where compute, storage, and networking technologies hosted by a third-party provider is offered to consumers' when requested without hesitation.

Low risk. A limited adverse effect where degradation in mission capability for a limited duration to the extent the business can continue to perform its primary functions. However, a reduction in the effectiveness of the functions occurs. This results with possible minor damage to organizational assets; and or minor financial loss (NIST, 2004).

Large enterprise. Gartner (2018) defines medium to large businesses with specific attributes. A business with more than 100 employees or revenue above \$50 million but less than \$1 billion fit the category of medium to large. For this study, the use of Gartner's definition of businesses includes medium or large businesses.

Moderate risk. A severe and adverse effect where significant degradation in mission capability to an extent and long duration in which the business can perform its primary functions.

However, a reduction in the effectiveness of the functions of the business occurs with significant damage to organizational assets or significant financial loss (NIST, 2004).

Platform as a service (PaaS). PaaS is a valuable service offering that enables the business to run applications on the internet, creating increased business productivity. Gartner (2018) defined PaaS as a service offering from a third-party provider of cloud services as a software middle tier or layer between the SaaS and IaaS layers of cloud service offerings.

Risk. Gartner (2018) specifies IT risk in its definition. The Gartner definition utilized for this study, as stated, a possible unexpected and adverse business consequence involving failure or misuse of resources.

Service level agreement (SLA). Gartner (2018) provides this explanation for SLA, SLA is an agreement between a service provider and a purchaser setting expectation and recitation of the services or products to be provided.

Service Provider. The provider of the cloud or federated services for this study included one provider of cloud or federated services, limited to either Microsoft Azure or Amazon AWS.

Software as a service (SaaS). SaaS is the current delivery model for internet published software that enables the business to adapt and adjust with rapid success to changing conditions and enable their customers to do the same. Gartner (2018) defined SaaS as a common software set to standard specifications that are delivered and managed by a third-party provider, consumed by customers through subscription.

Assumptions and Limitations

Assumptions

Several assumptions existed in this qualitative case study. The first assumption was that participants would be truthful and honest in relaying their experiences about risks and cloud

migration. The second assumption was that the participants would respond in a positive way to the interviewer and the interview questions. The third assumption in this study was that themes would emerge from the interviews with the participants and other sources of data. A fourth assumption considered that all participants would have had a significant part in this study's premise of migration to cloud services for their organization. Another assumption was limitations or errant issues as a part of the design of this study. This assumption included the study interview questions or issues which arose from the participant's answers. This assumption allowed the correction of the identified issues in the process to the betterment of the interview process. The final assumption was that this study was the data collection process. The interview process occurred over time, which provided the ability to process the data and validate it against the research questions. If the data collection process exceeded the predefined set time, a restructuring of the process occurred to mitigate the time lost.

Delimitations

This study can encompass the entire realm of all organizations around the world that use technology. There are too many delimitations to list for this study. The delimitations chosen to provide the best outcome for this study include geography, business type, experience, cloud computing, and risks. The utilization of this set of delimitations narrows the scope of this study and provided efficiency in gathering the research. This delimitation section clarifies the reasons for delimitation.

The geography or area of the world will be consistent with the area most considerable and familiar to the research, the United States of America. The significant number of entities that meet the criteria, including the size and type of business of this study make the choice of this geographic area optimal. The researcher's native spoken and written language is English. The

ability to conduct this study using the English language without a translation would reduce issues of error and omission. Further, the consideration of English as the only language for conducting the interviews was a consideration for this delimitation.

The application of interpolation concerning the business category applied across multiple industries producing findings in this delimitation. The size of the businesses chosen was medium to large enterprises using the Gartner (2018) definition. The type of businesses chosen as a part of the delimitation was to be businesses that use enterprise software. Business firms that use enterprise-level software provided a high level of relevance to the research question.

A major delimitation created by this study was the constraint to research businesses that were using the public cloud as a part of their migration. The overall diversity of the cloud offerings from vendors has increased during the timeframe used to compile this proposal. The choice to use public cloud offerings was to provide the findings of this study and make the research applicable to the largest census of businesses that will migrate to cloud computing.

The farthest period for data collection was no further than 5 years from the date of the research. The criteria for 5 years provided a delimitation for this study. Yin (2014) asserted that the information for case studies should be topical and relevant. By choosing this time frame, the information was topical and relevant, following best practices. Going beyond a three-year timeframe could cross into different experiences as cloud migration evolves. Capturing data closer to the date of the research data capture provided differences due to the cloud service model maturing.

Limitations

There existed various limitations within this qualitative case study, including the scope as related to geography, bias, population size, and interview questions. The first limitation of this

study included the scope. Limiting the scope in this study consisted of data from a small population consisting of participants from three businesses. The second limitation of the geographical area of the business provided information only from businesses in the United States. Further narrowing the location to the United States provided possible skewing of the data based on attitudes due to the nature or prevalence of migration patterns in the United States. Third, the population was small in size, which was a limiting factor even though the areas of perspective will be from multiple areas within each business. Fourth, the interview questions were limiting. The goal of achieving a thick description was possible. However, it was possible to miss this objective. The initial direction of each question precluded the participant's responses and refocused the interview. Fifth, the limitation of bias exists in almost all research, both from the interviewer as well as the interviewee. It was the interviewer's responsibility to create a neutral atmosphere. Providing an inviting area for discussion produced the most natural and least limiting observations from the participants. A sixth limitation was a bias from either the participant, the interviewer, or the combination of both providing data that was inaccurate. The seventh limitation pertained to the researcher's limited experience in conducting interviews of this type. The eighth limitation of this study was due to historical nature. No observation was possible from this study perspective. The events happened in the past, making research observation impossible for this study. A final limitation was the subject matter itself, the risk of the engagement as lived by the participants. Participants providing information may have a perception of the information they provide was unflattering or negative and refrain from providing accurate information.

Organization for Remainder of Study

The remaining sections of this study consist of the literature review, methodology of this study, collection, and analysis of data, and the presentation of the results. Chapter 2 provides a reference to the various works used for this study. Chapter 3 provides the methodology and insight needed to conduct this proposed study. Chapter 4 outlines and presents the results gathered through this study. Chapter 5 provides discussion, implications, recommendations, as well as further areas of research and an evaluation of the information provided throughout this study.

CHAPTER 2. LITERATURE REVIEW

Introduction

Yin (2014) stated that in the performance of a case study, a thorough literature review is a necessary basis for formulating a research question. A presentation creating clarity regarding the issues of the cloud migration paradigm and the management of risks encountered occur in this study. This literature review presents pertinent information from articles and industry information, including periodicals, all of which provide relevant information for this study.

Chapter 2 presents the relevant contemporary literature related to the research question of this study. Progression from cloud computing through the methods and designs which make up this study is present in Chapter 2. The information of Chapter 2 presents in three areas, including cloud computing, theory, and methodology. The first area presents cloud computing, migration, and risk. The second area has four segments consisting of risk, decision, change management, and the framework of this study. The methodology and design of this study are the final matters of discussion in this chapter. The Chapter 2 summary contains an analysis of the literature and the effect it has on the IT industry-specific to the topic of this study.

The literature assessed as a part of this literature review began through simple internet searches using conventional search engines, Google, for example. Using internet searches in this way retrieved large quantities of sources from the internet. These results included industry periodicals and works. The search for works included additional search engines and databases such as Google Scholar, ProQuest, ABI/INFORM Collection, ACM DIGITAL LIBRARY, and

seminal reference books. The terms used to search the literature included *case study, change management, cloud, cloud adoption, cloud migration, cloud computing, decision theory, framework, governance, IaaS, implementation, migration, NIST, PaaS, qualitative research, risk theory, risk management, and SaaS*.

Using selective criteria limited the results to less than 5,000 samples to navigate for this study. Adding criteria that eliminated journal articles older than ten years from the date of collection further reduced the literature samples. Decreasing the timeline parameter to three years further reduced the literature samples for this study. The literature included multiple physical books, with the remainder consisting of electronic versions of journals and research articles.

Chapter 2 provides a review of current and relevant literature consisting of three areas. First, literature that provides influence to this research study, including research, practitioner, and other supporting artifacts, are included. Second, literature that provides practicality for this research demonstrating value for both scholar and practitioner. Third, a review of literature that provides the basis for the theoretical framework used to analyze the data collected as a part of this study. Finally, an evaluation of the pertinent literature from the practitioner and theoretical perspective was present.

Review of the Literature

Cloud Computing

Cloud computing is reaching levels of acceptance on par with co-located data centers (Gartner, 2017). Migration to cloud computing is on the rise and is increasing (Bartoletti et al., 2017). The NIST (2011) comprehensively described cloud computing. The current cloud computing environment allows businesses the ability to take advantage of technology resources

suited to their specific needs using layers of abstraction quickly and efficiently without the burden of managing the underlying infrastructure provided through the cloud service provider (NIST, 2011). The basic conventions that compose cloud computing consists of (a) on-demand and self-service provisioning, (b) network access, (c) rapid and ease of scalability, and (d) measurability of use. These conventions are the minimum components for providing cloud services (NIST, 2013). This study uses the NIST (2013) definition and description of cloud computing.

Cloud computing is the distribution of technology endpoints. One business hosts infrastructure for another business on the internet (Abbadì, 2013). Businesses today have IT infrastructure co-located in data-centers similar to cloud computing. Co-location is different from cloud presence based on the ownership of the hardware and software. Businesses who own the hardware and software but not the facility which houses it is as defined as co-located, where the business that has an agreement with a service provider for the software and the underlying hardware with no ownership only the use rights are cloud-based (Jennings & Stadler, 2015). The similarity between co-located servers and cloud services ends where the consuming business uses the services provided in abstraction (Kushida et al., 2015). The business does not need or know what the underlying infrastructure is (Kushida et al., 2015).

Cloud computing is not a new technology. Cloud computing is over a decade old (Kratzke & Quint, 2017). What is new is the transformation to a complete service architecture (Kratzke & Quint, 2017). Service architectures change the way business firms utilize and pay for technology (Patrignani & Kavathatzopoulos, 2015).

The benefits of cloud computing are well known touted by anyone associated with cloud services (Vision Solutions, 2017). Cloud computing benefits include resource sharing, cost

savings, business optimization, scalability, the elasticity of resources, application security, identity, and access management, to name a few (Rahman et al., 2017). The opportunity to take advantage of such benefits comes at a price.

Business firms have, by tradition, used capital expenditures (CAPEX) to pay for significant IT endeavors (Patrignani & Kavathatzopoulos, 2015). Today cloud computing is paid for as an operational expense (OPEX) (Patrignani & Kavathatzopoulos, 2015). Before cloud computing, businesses estimated the size of the infrastructure needed for operations and purchased the equipment (Link & Back, 2015). The cloud computing model provides the business with IT resources. When more resources are needed, additional resources are purchased and applied immediately, enabling the business to scale (Fahmideh & Beydoun, 2017; Schneider & Sunyaev, 2015).

Cloud computing is continuing to mature (Gartner, 2016; ISACA, 2014). The types of offerings from cloud service providers are an evolving landscape (Bartoletti et al., 2017; Vision Solutions, 2017). Cloud computing is the new paradigm for businesses that understand the use of technology as a resource and how it is advantageous (Domínguez-Mayo et al., 2015; Gartner, 2016). However, full or even partial migration of cloud computing requires a significant change in the business approach (Alkhalil et al., 2017; Căţinean & Căţdea, 2013).

The NIST (2013) definition of cloud computing is consistent across the different types, including private, public, and hybrid, which are all referred to as cloud services (Căţinean & Căţdea, 2013). Each cloud model has characteristics and functionality features that are both detracting and supporting (Gutierrez et al., 2015). Multi-tenant cloud services have shared resources and the lowest cost, where private cloud services are the most expensive and use separate resources with hybrid somewhere in between (Gutierrez et al., 2015). Public cloud

computing has become the term in use by mainstream media when the discussion of cloud computing arises as a topic (Goel, 2015). Public cloud computing consists of network sourced, scalable, and retractable, and distributed computing platforms and is the standard environment available (NIST, 2013). The public cloud category of cloud services describes the original multi-tenant form.

Vendors continue to provide new cloud models within the current expansion of cloud computing. Resellers are creating new and novel coined terms that confuse the cloud services landscape (Bartoletti et al., 2017). The standard models which cloud services fall into are one of three typical silos: (a) software as a service, (b) infrastructure as a service, or (c) platform as a service (NIST, 2013). Exceptions and one-off derivations of these models exist as well.

The initial cloud compute model started as three offerings consisting of software as a service (SaaS), infrastructure as a service (IaaS), and platform as a service (PaaS) (Domínguez-Mayo et al., 2015; Ray, 2016). These tenders were the beginnings of a new exemplar in distributed computing (Jennings & Stadler, 2015). The benefit for an organization to migrate to cloud computing is from the cost savings with not having to purchase commoditized hardware and support infrastructure (Kushida et al., 2015). The previous methodology for IT infrastructure is purchasing outright using a capital expenditure approach. Cloud computing changes the paradigm for IT infrastructure from a capital expenditure to a subscription-based pay-as-you-go model (Attaran, 2017; Farah, 2015). This change to IT infrastructure moves to operational expenses changing the business financial structure of IT (Kushida et al., 2015).

This literature review has many articles and works that provide original as well as relevant information for this study. Yin (2014) asserted that a literature review should continue until recurring themes exist. When the discovery of new information pertinent to the topic

ceased, this literature review ended. The following section provides highlights of these works as they pertain to the research conducted as a part of this study.

Zota and Fratila (2013) provided that cloud computing is becoming the standard for off-premise business practices. Zota and Fratila further assert instances of European countries use standardized practices for cloud implementation differently than those in the United States. A comparison between the European businesses and industries in the United States is possible using these standards. A majority of the recommendations involve enterprise planning for the acquisition of cloud growth, not recognizing smaller organizational needs to expand to the cloud.

Guidelines exist in cloud computing, which applies to any industry and could be the basis for standards in cloud governance (Casassa-Mont, Matteucci, Petrocchi, & Sbodio, 2015). Casassa-Mont further suggested the interaction between both individuals and organizations and the respective providers of the cloud services are aligned. Included are specifications regarding contract requirements, service level agreements, and data sharing covenants, among others.

Casassa-Mont et al. elaborated on data regarding the use of information. Examples include the way the owners of the data and the cloud providers provide consumer use of the data. Casassa-Mont et al. provided that the use of ITG is vital as it pertains to management's use of cloud assets and the controls on those assets. The presentation from the perspective of the end-user, as well as providers, occurs. Casassa-Mont et al. described a high-level view of ITG and its use towards the management of cloud services being central to the usage of IT controls.

Lynn et al. (2016) provided a point of view where trust of a particular opportunity in cloud computing outweighs or negates the need for ITG as it would be applied. Lynn et al. (2016) elaborated additional details where trust would bridge the gap, including where the possibility of governance is not possible. Lynn et al. (2016) asserted an opposite viewpoint in

identifying the need for ITG in cloud computing could be beneficial as an alternate point of view for contrast. Identification of the governance model is required. It is possible to supplant the COBIT® 5 governance framework stretching it into the cloud as a point of management and reference.

Schlosser et al. (2015) suggested information specific to ITG, relating business needs to the infrastructure is put in place by technology departments. Schlosser et al. (2015) asserted the role governance mechanisms play in handling both information and technology and space where both mesh and combined. The detail of governance roles and responsibilities as applied to technology in an organization create the governance model. The authority making decisions regarding governance both at a business level and at a technology infrastructure level is responsible for owning these decisions (Schlosser et al., 2015). Schlosser et al. (2015) described issues of social alignment between IT and business, and the applicability and overall benefit to most organizations with extensive technology use and background.

Mahy, Ouzzif, and Bouragba (2016) discuss information technology and governance. Mahy et al. (2016) presented how enterprise organizations using technology have technology governance to control and manage resources. Once a business reaches the size of two practitioners, the use of governance becomes a necessity even if informal governance is practiced (Mahy et al., 2016). Core insight into ITG and the boundaries organizations operate in are outlined. Mahy et al. (2016) further provided insight into how businesses implement governance using standards such as ITIL and COBIT methods and principals and frameworks. The methods that describe ITG provide core reference information. The follow-on sections for other methodologies account for comparison and contrast to technology governance.

Crampton (2015) discussed information on data, big data, and governance along with the issues of privacy and protection of data and the issues associated with security. Crampton (2015) further discussed multiple references to specific security realms. The ability to reference core sources that bind together governance with security is key to creating valid IT controls (Crampton, 2015). The information provided by Crampton (2015) is not derivative and applies to cloud computing but brings about security and governance at core technology levels.

Debreceeny (2013) suggested the different risks and values associated with IT governance and its value as applied to organizations. Debreceeny (2013) provided standard frameworks and models used in ITG. The use of the models and frameworks provide a base or core for future examination whether governance exists. Debreceeny (2013) did not reference remote computing when he discussed IT governance and risk. However, the same outlines that form the models used for IT governance apply to remote data, storage, and compute. Debreceeny (2013) outlined excellent references and areas for future research regarding ITG.

Pick (2015) provided a general overview of IT governance and how organizations need to meet the expectations of the business users but empower IT departments to control technology resources (Pick, 2015). Pick (2015) demonstrated the struggle between implementing governance and the usability of resources based on minimal guidelines of the business process. The IT governance needed to provide oversight and the adjustments that have to be considered by the organization to not stifle the operation both from a business perspective and a technological, logistical level through the use of ITG based on a top-down approach. Pick (2015) suggested that core management traits, as applied when working on governance issues, exist in most businesses.

Kajiyama, Jennex, and Addo (2017) presented information governance from the perspective of public e-governance rather than privately held entities. Kajiyama et al. provided the application of cloud resources as well as their scalability. Kajiyama et al. suggested the need to manage and control these resources in the cloud, similar to the way an on-premise infrastructure maintains them.

Kajiyama et al. (2017) discussed the sensitive issues, including the type of information stored as a part of government data that requires extra layers of security. Additionally, data stored in industry-standard shared cloud services has not required the same level of security. The authors presented the concept of different types of cloud mechanisms. Next, the authors presented characteristics of onsite versus offsite federation of infrastructure. Finally, the authors discussed the complexity of federated infrastructure and its higher than routine management and administration requirements (Kajiyama et al., 2017).

Kajiyama et al. (2017) asserted that different types of data require different types of security. The security requirements for each type of data determine the level of security used for each type of data. The governance required by governmental and legal mandates determines the security requirements for data. Each agency provides the controls that govern the security of their data.

Doherty et al. (2015) provided another look at the various barriers companies have in moving to the cloud, including the missing components of ITG. This study is somewhat unique in the approach the researchers took. When looking at businesses in the United States versus SMB's in Ireland, consideration of the author's quantitative methodology belongs in comparisons between the two. Doherty et al. (2015) expressed factors governing cloud-based federated architecture that exist that apply to all organizations throughout the world.

Jennings and Stadler (2015) provided a perspective of the cloud from the management of resources. Jennings and Stadler (2015) further discussed the appropriate allocation of such resources regardless of ITG in a shared environment. Further elaboration of the framework developed to handle resources in shared environments provides a unique vision for the management of resources. Jennings and Stadler (2015) next discussed the use of decentralized governance in shared cloud environments. The section on further research includes the development of quantitative metrics by resource allocation in the cloud used to generate further research methodologies (Jennings & Stadler, 2015).

Cloud Migration

Many challenges exist in the migration to the cloud computing paradigm (Alkhalil et al., 2017). The challenges include business, technological, statutory, cost, risk, as well as numerous other factors (Battleson et al., 2016). The benefits of business and technological practicality versus the cost of cloud migration are well documented (Cho & Chan, 2013).

The literature on the actual management of risks during migration to cloud computing is non-existent. The focus of other researchers has been on models and frameworks to observe cloud migrations (Karunakaran, Krishnaswamy, & Rangaraja, 2015). Domínguez-Mayo et al. (2015) described in detail the various areas surrounding cloud services and the frameworks and methodologies used to make decisions. Battleson et al. (2016) asserted that businesses need help and are looking for direction when it concerns migration to cloud computing. Karunakaran, Krishnaswamy, and Rangaraja suggested while prevalent in the literature on cloud computing, and significant areas exist that need further study, including the risk of cloud migrations.

Islam et al. (2017) stated, "No comprehensive risk management framework supports an organization by identifying potential risks before considering cloud adoption" (p. 4). The

statement made by Islam et al. is an appeal for research to be performed to gather risks associated with cloud migration. Using the framework from Islam et al. will build upon works already completed providing future frameworks of IT risk. Islam et al. are reiterating the sentiment of Karunakaran et al. (2015) that suggests the literature is still absent on this crucial subject.

Domínguez-Mayo et al. (2015) suggested that businesses, when adopting cloud computing and are tempted to move to an off-shore provider, must be observant of the maturity and capabilities of these providers. A necessity exists for a framework that validates risk as it is observed and encountered and provides a way for management. A single point of reference does not exist that a business can rely on by itself (Domínguez-Mayo et al., 2015). The observation of risk in cloud computing by Domínguez-Mayo et al. suggested further research into models of analysis for providers and the management of risks be studied.

Articles exist in the academic literature that detail decision capabilities surrounding cloud computing using frameworks for migration (Fahmideh & Beydoun, 2017; Mackita, Shin, & Choe, 2019). The literature contains lists of factors relating to cloud computing migration. Alkhalil et al. (2017) provided a more comprehensive list of risks aligned with businesses that can determine the cost-benefit of cloud migration. The list of risks provided by Alkhalil et al. is not all-inclusive of the actual risks incurred during the process of migration to cloud computing (Alkhalil et al., 2017). Alkhalil et al. suggested a general list of decision points for the process a business should consider for cloud migration.

The issues encountered during cloud computing migration are tradeoffs when compared to the monetary benefits provided (Ray, 2016). The perceived or real savings returned from migrating the enterprise infrastructure into an environment owned and operated by an external

vendor have different perspectives in a business (Carcary et al., 2013). There is a change made by businesses managing IT environments once the business has migrated to the cloud (Gartner, 2016). As an example, a change happens in the way businesses manage infrastructure with governance. Cloud computing management is different from self-managed environments due to the service providers existing governance model (Aleem & Sprott, 2013). Relying on service providers' governance does not include the use of standard controls and governance mechanisms (Von Solms & Willett, 2017).

As cloud computing becomes standardized, more businesses will migrate to cloud services (Bartoletti et al., 2017; Gartner, 2018; Vision Solutions, 2017). The lure for businesses to migrate to cloud computing is the significant savings touted by cloud service providers as well as other businesses (Alkhalil et al., 2017; Rahman et al., 2017; Vision Solutions, 2017). Gartner (2016) asserted that by 2020 25% of the IT market would be cloud computing. The significant amount of businesses migrating to cloud computing suggests that standards are occurring.

There are many questions about which method of cloud migration, as well as what framework will come to the forefront (Islam et al., 2017). Domínguez-Mayo et al. (2015) suggest that the e-SCM framework that values the maturity level of cloud providers offers significant value to businesses utilizing it. Domínguez-Mayo et al. declared while the e-SCM framework completes part of the ability for evaluation of cloud computing migration, no single reference framework that aligns cloud migration and maturity. Lack of maturity in cloud computing related to ITG is consistent with Debreceeny and Gray (2013) assertion for the study of ITG maturity in other IT paradigms.

Cloud computing boundaries fall into one of three spaces private, public, and hybrid (Farah, 2015). Each segment of the cloud service offering provides a delivery or consumption

method or both (NIST, 2013). Businesses positioned in one of the three segments private, public, or a hybrid of private and public make up the typical adopters of cloud computing (Căţinean & Căndea, 2013). The best-known segments of cloud computing are public, private, and hybrid (Căţinean & Căndea, 2013). This study, while identifying and providing a review of these areas, will focus on the public segment of cloud computing.

Migration Risks

The risks encountered in cloud computing are numerous. Cloud risks overlap those of on-premise IT. Gartner (2017) suggested the risks associated with cloud computing be identified and mitigated as a part of adoption within their framework. Rahman et al. (2017) provided a comprehensive framework, including both decision and business alignment, for cloud migration use by enterprise businesses. Rahman et al. (2017) further described technology risks associated with migrations with security at the top of the list.

Cloud computing risks overlap those of on-premise or co-located IT infrastructure as well as others unique to the cloud paradigm (Islam et al., 2017). Cloud computing introduces new risks outside the standard security, privacy, governance, and availability risks. New risks include vendor viability, compatibility, and application portability, to name a few. A need for a more comprehensive list of risk categories consistent with cloud migrations exists (Islam et al., 2017). The risk of migrating to cloud computing is intrinsic (Rahman et al., 2017). Migrating to cloud computing is complicated for business. Evaluating the benefits of migrating to cloud computing compared to the risks involved is a necessity before starting a cloud migration. If a business is unable to migrate to the cloud successfully, they risk loss within their market (Gartner, 2016). It is also possible for a migration to the cloud to cost more and expose the business to negative results. New risks are found based on the cloud computing model (Islam et al., 2017). New

cloud computing risks include areas of multi-tenancy, elasticity, data leakage, exclusive provider agreement, and enterprise governance non-compliance. These risks could outweigh the benefits of migrating to cloud computing (Islam et al., 2017; Rahman et al., 2017). Adverse outcomes exist for failed cloud migrations with considerable financial costs (Gartner, 2016).

Technology risks that affect the business is an ongoing area of concern. Vision Solutions (2017) asserted that two-thirds of clients polled had postponed a cloud migration due to risk. The most frequent risks consist of security and data compromise (Căţinean & Căndea, 2013). Over time the maturing of cloud computing will reduce risk (Ray, 2016).

Other risks business firms face when migrating to cloud computing is the availability of systems (Karunakaran et al., 2015). Availability regarding technology concerns two issues. First, providing the internal business with access to vital systems once migrated to the cloud. Second, the provision of external customers using services migrated to the cloud. An internal, as well as an external risk, now exists. Each risk has equal concern for the business. Both availability concerns are affected by the cloud services provider.

Businesses utilizing their internal cloud applications and data have a critical dual dependency on their cloud service provider (Dantas, Matos, Araujo, & Maciel, 2015). The availability of the business to customers is vital for reputational issues (Alkhalil et al., 2017). Loss of availability is a risk as crucial as security. Availability to the business applications and data is the highest priority when a business migrates to the cloud (Cámara, Fuentes, & Marín, 2015).

Risk Theory

Risks are a fundamental driver for managing decisions in both social circumstances as well as a business (Slovic, 2016). Businesses use risk management in information technology as

a fundamental tool (Slovic, 2016). Risks imposed on information technology through the business occur similar to external risks. Risk versus reward is a shaping factor in the evaluation of risk. Risk versus reward includes the decisions and choices in technology businesses.

IT risk defines a possible and unintended occurrence, including a failure or mismanagement of IT resources that would place the business's goals in threat (Westerman & Hunter, 2007). Multiple types of risks exist in information technology implementations (Ray, 2016). The risks associated with technology are diverse (Alkhalil et al., 2017). Subtle differences exist between technology risks and business risks. Each type of risk provides the opportunity to threaten the business (Rahman et al., 2017). Misalignment between the business and technology increases the threat of each risk (Jana & Rudman, 2019). The business firm is the definitive owner of all risks.

The literature has comprehensive documents of areas of risk. Multiple frameworks with decisional routing based on risk exist (Nicho & Khan, 2017). The most significant as well as prevalent risk to IT in the cloud is the security (Battleson et al., 2016; Cho & Chan, 2013; ISACA, 2014). Security in the cloud is one of the many possible risks of cloud computing.

During the collection of artifacts for this study, numerous instances of security issues occurred. The Equifax security breach, which occurred in 2017, is an ideal example of cloud security risks (Andriotis, 2018). The Equifax security risk exposed more than 145 million consumers and their personal information in the United States (Andriotis, 2018). The Equifax breach is one of many types of security risks that exist.

Further risks include financial, legal, operational, reputational, as well as others. Each area of risk has distinct characteristics. Financial risks include unforeseen or uncontrolled events that include unexpected costs or monetary loss (Slovic, 2016). Other frameworks exist specific

to the areas of operations, financial, legal, and general governance for cloud computing (Gartner, 2016; Rahman et al., 2017).

Most risks affect private and public-sector businesses equally. Both utilize similar types of governance, with the only variance on the focus. The private sector businesses focus on the identification and prevention of financial and operational risks (Wilkin, Campbell, & Moore, 2013). The public-sector agency will look to identify and prevent political risks.

Decision-makers within a business make selections based on their cultural backgrounds, bias, and experience (Slovic, 2016). In the same way, agent experience provides a perception of each risk. The agent uses this perception in their assessment of each risk. The agent's perception defines the level each risk poses to the business. Agent perceptions and biases affect the decisions for the business (Westerman & Hunter, 2007).

Risk perception occurs at multiple levels from a micro to a macro standpoint. Misinterpretation of a known threat is significant. Inexperience or ignorance can be detrimental to risk assessment (Markolf, Klima, & Wong, 2015). It is possible to contrast a lesser threat having greater exposure versus a more significant threat with little to no exposure to the business (Slovic, 2016). A comparison is possible when an agent is unable to comprehend the outcome due to ignorance (Slovic, 2016).

Slovic (2016) further suggested how risks are encountered or presented changes the perception of the risk. Business risk governance occurs from the perception at high levels within an organization, which causes a process transformation (Westerman & Hunter, 2007). As an example, an IT risk archetype such as connectivity. This risk has multiple presentations; the network is down, the server is offline, the internet connection failed. Perceptions of this risk are different between IT and the business.

The basis of risk perception occurs in the presentation. An example of a negative perception is a risk with a recognized with a 50% rate of failure. The same risk demonstrated where half the phenomenon is successful is perceived to be positive (Slovic, 2016). This description is analogous to the glass if half empty versus half full expression describing optimism or pessimism. The experience of the decision-makers creates a significant role in risk management between positive and negative perceptions.

The study of risks in business arises in great detail historically. General risks have parameters that are succinct and limited in concentration. The study of risk as a modern phenomenon applying probability and consequence creates the model for risk (Slovic, 2016). The combined factors of consequence and probability together make the generalized idea of risk visible (Westerman & Hunter, 2007).

The idea of risk is different from the perception of risk. Perceived risks include bias, experience, knowledge, into the concept. Removing bias does not provide for a nonappearance of occurrence. The move from a general concept of risk to a specific divergence of an actual event remains (Slovic, 2016). Understanding risk is a possible occurrence that has not happened is a key concept (Sankararajan & Shrivastava, 2012). Alternatively, an issue is a risk that has become a problem (Sankararajan & Shrivastava, 2012).

Risk is a significant factor in the decision process that requires identification of the risk (Islam et al., 2017). Decision theory is a part of risk management (Jaeger, 2016). The alignment between risk theory and decision theory can be different (Eastburn & Sharland, 2016). Risk theory complements decision theory when the two operate together to provide an outcome. Understanding the frequency of events intertwined with risk unencumbers the decision-maker through the consideration of remuneration achieved versus the risk taken to achieve the goal

(Slovic, 2016). Westerman and Hunter (2007) suggested that risk origins do not have a relationship with a single technology but exist due to inadequate business governance.

Risks exist, and all migrations encounter them (Islam et al., 2017). The term risk, when used in this research study, has four areas. The first area of risk is the identification or recognition of risk. The second area of risk defines the risk and the threat level it poses. The third area of risk identifies if the risk is known or unknown. Known risks are preferred risks previously examined. Unknown risks are less favorable than known risks. Unknown risks should be cataloged and a method to dispatch created when possible. The fourth area of risk considers the management or mitigation of the risk itself. Can the risk be avoided? If it is not possible to avoid the risk, what process will the business use to mitigate and reduce the effect on the business? Preferred or known risks are desirable even at a higher threat than unknown risks posing a lesser threat.

Decision Theory

Human beings make hundreds of decisions a day, for example, “I will have coffee this morning with my breakfast.” Berger (1985) asserted decision theory as a conundrum of making decisions. Decision theory in the literature refers to statistical decision theory. Statistical decision theory is producing a decision with statistical knowledge (Berger). Further, Bayesian decision theory is concerned with producing decisions in situations of ambiguity with estimation (Meier, Favero, & Zhu, 2015).

One of the primary sources for decision theory is Herbert A. Simon. Simon (1997) created multiple seminal works on human behavior, including bounded rationality, administrative behavior, and the sciences of the artificial. The works of Simon have provided the foundation for multiple scientific domains, including administration, economics, and

business (Buchanan, 2008). This study uses Simon's works as well as later works that added to and built upon his seminal research.

Looking at decision theory from many perspectives as possible creates an area for analysis. Analysis of information, including risk with uncertainty, then applying statistical decision theory, can reduce mistakes (Vidal, Rodríguez, Campdesuñer, & Vivar, 2017). Elezi and Bamber (2018) described decision making, using multiple models as a framework to understand organizational decisions. Bromiley, McShane, Nair, and Rustambekov (2015) asserted that enterprise risk management (ERM) from the beginning stages needs decision theory as part of a complete process. Lundqvist (2015) goes further, having asserted risk governance is a merger of business governance and risk management and the identifying trait of ERM.

Of the seminal works of Simon, *The Sciences of the Artificial* provides refinement of decision theory into the business application (Simon, 1955, 1996). Simon asserted that statistical decision theory is a utility and can be used to form a framework to observe choice. Decision theory describes the observation of agent choice using knowledge with or without estimation to create an optimal outcome (Berger, 1985; Simon, 1955). Simon described Bayesian decision theory as an add-on of decision theory based on both probability and estimation of the decision-maker using previous information to alter the decision.

Simon (1955) described another area of study, the science of design. Design theory adds to decision theory by including areas of management and organizational theory (Buchanan, 2008). Buchanan provides a contemporary perspective on design. Buchanan's work moves from decision making into design thinking into the practice of design rather than the action of design (Buchanan, 2008). Buchanan is in contrast to Simon about design theory. Buchanan

asserted that the application of decision-making is best through design thinking on other domains (Buchanan, 2008).

Change Management Theory

Kurt Lewin is the seminal author of change management theory (Cummings, Bridgman, & Brown, 2015). Lewin reduced the process of change in business to a three-stage process (Sarayreh et al., 2013). The stages of the Lewin model are (a) unfreeze, (b) change, and (c) freeze (Sarayreh et al., 2013). Businesses can move from the technology state of localized ownership and management to another state of vendor managed infrastructure using controls and governance, including change management to minimize disruption (Cummings et al., 2015).

Lewin considered human behavior during his design of the stages of change management (Lewin, 1947). Lewin's three stages of change management, while simple in design, provides ease of management for businesses of all sizes (Seethamraju, 2014). The first stage, unfreeze, puts the business on notice a change is coming. Stage one provides a communication process that affects human behavior setting expectations and aligning the expected outcome for the business (Lewin, 1947). The second stage is the change to the business. A change could be as simple as a software patch that changes daylight savings time on computers to something as complicated as a new data processing standard with hardware software and training. The third and final stage of Lewin's change model is solidifying the business in the new state after the change has occurred (Cummings et al., 2015). This stage is the freeze stage that allows the business to resume working regularly.

Change management is a standard business process. The use of change management provides for the enhancements and modification of technology (Sarayreh et al., 2013). A business that has multiple employees performing different duties is at risk when making systemic

changes (Seethamraju, 2014). Lewin's simple model allows businesses to control the process of change (Sarayreh et al., 2013). Using the change management model accomplishes three purposes. Communication with all involved parties in the business change is coming and settings expectations. Controlling the organization and using a process for making a change in the business. Business firms utilize change management to minimize and control disruptions to the business operations to accomplish business goals (Sarayreh et al., 2013). Finally, the business is brought into a working state after the shift has occurred.

It is possible to construct a framework to evaluate the decisions of an organization using the three stages of change management. Planning and research occur in the first stage. Following the first stage, the decision happens in the second stage. Finally, stage three is the evaluation of the decision and a reflective look at the process. Expansion of each stage could include other sub-areas of the emerging themes of decisions. As an example, the expansion of stage two will evaluate the process involved before the decision, including the constraints, risks, and benefits, and any factors during the stage that would affect the outcome.

Theoretical Framework

There was an examination of many theories for this study. Theories and models considered for use in this study underwent an examination for alignment with the topic and research question. The theories aligned with this study align with management and decision making, as well as risk. The change management process, decision theory, and risk management theory best aligned with the research question. The ability to create a framework from these three theories existed. The three theories or models examined for use in constructing the conceptual framework for this study have strengths and weaknesses. The examination of each theory or model included their benefits, constraints, as well as possible shortcomings.

First, an examination of Lewin's (1947) change management theory and model occurred. The model of change management is the outline of a process organizations use to alter or transform existing paradigms (Lewin, 1947). The constructs consist of three conditions (Lewin, 1947). The first condition is the organization as it exists (Lewin, 1947). The next condition is the organization in transition to a new state of being (Lewin, 1947). Finally, the last condition is the completed form of the business when the transition is over (Lewin, 1947). The common practice of the change management model process has the following stages unfreeze, change, freeze.



Figure 1. Change management method.

The simple three-stage change management model would be easy and fast to generate a framework for the observation categorization of decisions and management, as depicted in Figure 1. While small and robust, change management would create categories too general for some themes of this study. The alignment of change management as an underlying model for the conceptual theory for this study is adequate. Using change method theory does not provide as robust a categorization or coding scheme as decision theory or risk management theory.

Next, consideration of Simon's (1996) decision theory for this study occurred. The constructs making up decision theory provide insight into human choice applied to a situation and include actions, measures, results, and settlements (Simon, 1955). Actions are the choices of an actor (Simon, 1955). Measures are happenings at the time of the actor's consideration of

possible actions to take (Simon, 1955). Results are the product of the combination of measures and the actions the actor took (Simon, 1955). The settlement is the weight of the results the actor considers when choosing actions (Simon, 1955).



Figure 2. Decision theory.

Simon (1955) crafted the idea of decision-making theory in the 1940s. Schindler (2019) asserted that rational decisions give the highest probability for a positive outcome. Simon further depicted decision theory using five categories, including understanding, definition, ideation, pilot, and evaluation demonstrated in Figure 2. The assertion from Schindler restates Simon's declaration regarding bounded rationality in the decision-making process. The decisions made in business are rational as well as aligned with the goals of the business (Cleary, & Quinn, 2016). Hill (2016) suggested that companies using agents for decision-making should employ ethical actors. A need for ethical consideration of business decisions exists; this requires governance as part of the process (Hill).

Decision theory, when not parallel to design theory, provides many of the same traits (Simon, 1996). Consideration of design theory overlaid on decision theory as an evaluation process occurred for this study. Using design thinking is an abstraction layer that presents the ability to create a framework to categorize themes using decision theory. The use of five concepts for design thinking to categorize the decision process of managing risks during cloud computing migration occurs.

Modern risk management evolved from insurance management after the Second World War (Dionne, 2013). Gahin (1967) asserted that two types of risks exist. Gahin goes on to elaborate that the first type of risk is Pure Risk. Gahin states that the only outcome of a Pure Risk is a loss for the business. Gahin explains that the second type of risk is speculative risk. He suggests that the outcome for speculative risk is either loss or possible gain.

Modern risk management has taken a middle-ground approach between Pure Risk and speculative risk (Dionne, 2013). The constructs that define modern risk management theory consist of observance of exposure, characterization, measurement, and mitigation of risks.

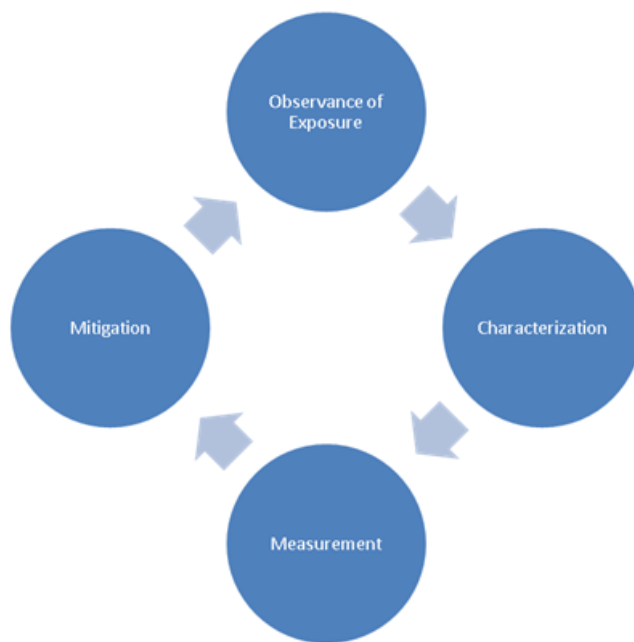


Figure 3. Risk management cycle construct.

Risk management theory is more of a cyclic process than the other theories identified in Figure 3. The use of risk management is challenging to use in human decision observation

outside of specific parameters. Using the constructs of risk management to create a framework for decision processing is problematic beyond risk management scenarios.

The first stage of the conceptual framework is understanding. The stage of understanding will categorize the earliest themes of this study. Concepts that are yet to be defined or even acknowledged would be listed here. The understanding stage is a catch-all for concepts before they move into the management process.

The process of defining the conceptual framework is the second stage. The definition stage is the first stage of the formal management process. The definition stage of the framework categorizes themes relating to design theory concepts. This stage will include concepts that were known and had a reoccurred or were unknown.

The third stage of the conceptual framework is ideation. This stage categorizes themes from this study concerning new concepts of the management process. The use of a concept that exists in a new or different way belongs to stage three. As an example, any free-flowing ideas that happen during the process would fall into this category.

The fourth stage of the conceptual framework is the pilot. Themes that belong in the pilot stage are any actionable assignments. This stage collects themes of action even if the actions are not new. A presentation of actions taken no matter the outcome happens at this stage. The fourth stage is for governance, recommendations, and assessments.

The fifth and final stage of the conceptual framework is evaluation. The process includes an evaluation of the process to validate that the expected outcome occurred with certainty. Further observation of processes to understand if the action taken worked is identified and noted with either a positive or a negative outcome. The placement of other results occurs in stage five. Any final thoughts, efforts, or evaluations from this study belong in this stage.

Conceptual Foundation for the Study

Methodological and Design Literature

The question this study is going to answer is how businesses manage risks during migrating to cloud computing and what processes they used. The literature on frameworks and processes, as well as their use, exists. The literature on cloud computing exists to a high degree, including migrations. Risks and risk management have no shortage of literature. However, no existing literature exists where the findings of a study that present the decisions regarding the management of risks during cloud migration. The use of a descriptive qualitative case study provides the most relevant and contemporary information for this study.

The design of this study was a case study. The use of a qualitative method has occurred for this study. The subject of this study is risks and the management process of those risks by the businesses during migration to cloud computing. This section of Chapter 3 will review the literature on the methods and designs this study uses. This review includes works from seminal authors and recent examples of reviewed literature.

Yin (2014), as a seminal author on case studies, provides the best practices a researcher should use in establishing their research study. The uniqueness of every study prevents an explicit criteria definition for all case studies. However, Yin described the areas where case study research is common, business being one. In particular, the use of case studies provides comprehension of complex phenomena (Christensen, Johnson, & Turner, 2020; Yin, 2014). Several indicators exist and are used to identify the correct methodology for a qualitative study (Creswell & Creswell, 2018; Yin, 2014).

Yin (2014) elaborated on criteria concerning exploratory, descriptive, and explanatory types of studies. The differences are subtle, exploratory presenting new information, descriptive

adding information, and explanatory presenting why something happened (Yin, 2014). Merriam and Tisdell (2016) stated descriptive designs analytically describe the proofs and features of a given phenomenon. Exploratory and descriptive work is in alignment with qualitative research (Creswell & Poth, 2016; Yin, 2014). Christensen et al. (2020) discussed the attributes of the case study regarding intrinsic, instrumental, and collective types. Intrinsic manifested as a study narrowed to the single case versus instrumental described as a general study not focused on the case versus the collective study comparing many cases (Christensen et al., 2020).

Yin (2014) suggested observation of the strengths and weaknesses of the case occur from the start of the study. Yin further expresses that case study method covering the issues of discovery in a historical case study is daunting. The issues of nuances missed by the researcher can create bias. As an example, information from items such as the notes of the study by the original author or the respondent's audio-recorded answers to the research questions, create a significant area for bias.

As the pool of literature increases, the capture of historical data becomes more challenging in parallel with the significance of the data. Providing adequate data points for reference and comparison makes the study more reliable (Stake, 2010). The case study design operates in concise parameters to provide relevant information (Stake, 2010). Stake further asserted that case studies observe the bounded subject of the study with strict examination. Information for this type of study can have a profound effect on the area studied (Creswell & Poth, 2016).

Capturing qualitative research happens in specific ways. One method for capturing qualitative data is through observation in a normal setting (Christensen et al., 2020; Creswell & Creswell, 2018; Yin, 2014). Capturing information from different vantage points of the business

provides different perspectives. Different perspectives provide context to the data where it is collected (Creswell & Creswell, 2018). The collection of documents from the business contributes to data validation. Different types of data, including interviews, observations, and documents from multiple sources, increases data validity and reliability through triangulation (Creswell & Creswell, 2018; Yin, 2014).

Analysis

The research question for this study relates to the primary subjects of cloud computing, management, process, and risk. Each of the primary topics of this study has a large number of papers in the literature. The literature reviewed for this study became predictable and repetitive quickly. Finding repetitive information on each subject with no new information demonstrated data saturation in the literature.

The literature provided for cloud computing in this literature review begins in the mid-2000s. Next, information detailing cloud computing as a technology platform occurs. Next, a presentation of an example describing the benefits and issues of cloud computing takes place. A presentation of the details regarding the type of businesses using cloud computing and those migrating to cloud computing exists in this review.

A presentation of cloud migration as a general concept occurs. A presentation containing a list of many common cloud migration risks exists in the review. Additionally, a presentation of frameworks and models used for cloud migration occurs. The identification of governance, process, and policy deficiencies in cloud migration is present. Next, the topic moves to the various areas of risk, which result in mitigation processes for cloud migration.

The definition of risk as a concept exists in the literature. Present in the literature is an association between risk and cloud computing. A presentation of risks that stand out in cloud

migration exists in the literature. Present in the literature, the difference between issues and risks as concepts occur. The differences between risks and issues lead to the process of management identified in the two concepts of risk and issues.

A presentation of the high point risks associated with cloud technology exists. The presentation highlights the most noted risk, which includes governance and security. Next general areas of remediation and mitigation occur. Next, a presentation of the processes associated with risk management occurs. Finally, a review of risk management specific to technology and cloud computing occurs.

A description of the management process occurs. This study includes the seminal theory of decision theory. This study presents decision theory as the basis for the conceptual theory. The ideas within decision theory are itemized and presented. Also, an outline of the key concepts of decision theory exists. The presentation of a framework derived from decision theory follows.

A presentation of change management as an alternate theory for this study occurs. This study presents change management as a process. The crucial areas of change management that provide observation points of management are listed. The idea of creating a framework from the change management theory is present. This study presents the benefits and detractions for the creation of a framework from change management.

This study presents the differences between change management and decision theory. The need for a framework used for this study is present. A description of the complexity of the research question compared to the lens of both decision theory and management theory occurs. The difference between decision theory and change management for building a framework is present.

The areas of cloud computing and risk management are present separately. The focus of the study on cloud computing and the management of risk processes during cloud migration is missing. The literature which demonstrates a need for this area of technology to be studied is present. The identification of both current and seminal works in different domains of technology, promoting the study of risk in technology happened.

The literature review presents a review of works that form the basis for the business problem. Alignment exists between the literature and the research question. A presentation of the methodology of this study spanning qualitative research with case study design occurs in the literature review. The seminal and current works that describe the research methods are present. Areas of research that are the underpinning for this study are present.

Conclusions

This literature review presented pertinent information from articles, white papers, case studies, and industry information. This review provides backing for the foundations of the research question in this study. The organization of this Chapter progresses from cloud computing to the methodology and design of this study. A review of the risks of cloud migration follows the section titled cloud migration. An examination of the theories that could provide a categorization of emerging themes for this study was present. These theories included the primary theory used for this study, Simon's decision theory, and design theory. Simon further provided information on institutional assignment and behavior, which was an addition to decision theory, in his works on administrative behavior (Simon, 1997). An alternate theory, Lewin's theory of change management was reviewed and presented. The change management theory trailed by the conceptual theory and framework created to observe this study and create

the necessary and appropriate categories for the emerging themes. A review of the methodological works used for this study was present.

Lastly, this Chapter presents an association between the research question formed and the literature reviewed for this study. The use of seminal works provides the foundation for the conceptual framework, including both decision theory and design thinking, along with the methodology of this study itself. Finally, the presentation of relevant information on cloud migrations, risks, risk management, decision theory, and a framework used to collate this study from the business firm's perspective based on its decisions during the migration to cloud computing is present.

CHAPTER 3. METHODOLOGY

Introduction

This chapter has eight sections beyond the introduction and summary. Chapter 3 of this study includes the following section's design and methodology, participants, the setting of this study, analysis of the research question, credibility and dependability, data collection, data analysis, and ethical considerations. Each section of this chapter presents relevant and pertinent information for this study. The sections are specific in scope but also draw from and add to other sections in Chapter 3.

Chapter 3 links the research to the activities performed in this study. The purpose of this study was to examine how business firms in the United States manage risks during migration to cloud computing. This chapter presents the specific actions, design, and methods used to collect data for this study. Chapter 2 presented a review of the literature, industry, seminal, and topical works included in this study.

Design and Methodology

This study was a qualitative descriptive case study. The case for this study is business firms in the United States who have migrated to the cloud in the last five years. The characteristics of this study include the observation of risk management processes during the migration to cloud computing. This study presents the findings of a detailed and thick descriptive nature of a complex event.

The research question and goal of this study was to describe the results of a complicated question using information collected from participants. The qualitative method was appropriate for this study. Looking at complex human issues can be accomplished using a qualitative method (Yin, 2014). The case study design and method are appropriate for this study, as the research question probes to describe a complicated situation. The qualitative method is consistent with case study design and methods. As described by Dennehy and Conboy (2019), the use of a case study qualitative method when witnessing business methods is both practical and valuable.

This study does not use phenomenological, ethnographic, grounded theory methods, or narrative inquiry design. This study does not present information on the story of an individual. This study does not offer data of a theory based on the actions of the participants. This study does not present the findings of cultural studies. This study does not show data on the lived experiences of the participants. Without the utilization of phenomenological, ethnographic, grounded theory methods, or narrative inquiry design, the method left for this research was a case study.

Many qualities are looked for when determining the best method for a research protocol or method. This study does not include traditional quantitative research properties, including a hypothesis, statistical analysis, experiment, or quasi-experiment. The presentation of data for statistical analysis does not occur, nor was a hypothesis proved or disproved. The use of quantitative research methods did not occur in this study. Absent the use of quantitative or a mixed-method research methodology, a qualitative research method was best suited for this study.

Participants and Setting

Participants

The criteria for the population of this study consisted of four qualifications. The first qualification was a business firm in the United States. Second, the business had to be at a minimum of medium enterprise business. In order to provide value, this study focused on information about enterprise businesses at or the medium-size. Medium-sized businesses have a workforce of employees between 100 and 1000, with less than 250 million dollars in annual revenue Gartner (2018). Gartner (2018) further describes large enterprise businesses with resources exceeding those of medium sized enterprise businesses. Third, the business had migrated to cloud computing in the last three years. Fourth, the business was using enterprise software in the cloud.

The participants for this study also met several criteria. First, each participant must have worked at the business firm during the migration to cloud computing. Second, the participant must have worked in one of three operational areas of the business during the migration to cloud computing. The three areas each participant must have worked included executive management of the business, IT management, or as an IT practitioner. Third, the participant must have had direct knowledge of the cloud migration process the company used. Finally, the participant must speak English.

Multiple criteria existed that excluded participants from this study. If the participant had no direct involvement in the migration to the cloud for this business, this excluded the participant. When a participant was not in one of the three operational areas, including business management, IT management, or IT, and exclusion from this study occurred. Finally, participants who did not speak English did not participate in this study.

Leedy and Ormrod (2018) asserted that purposeful sampling is to comprehend a precise circumstance. The choice of the population for this study was deliberate. Christensen et al. (2020) asserted that random sampling gives everyone the same opportunity to be a part of the research. Using a random sampling does not provide the best choice for success in researching the goal of this study. The researcher was aware of businesses that meet the population requirements for this study. The researcher asserts there was no influence over the businesses considered for this study. Extracting potential researcher influence of the population removes one ethical consideration. Purposeful sampling was appropriate for this study of experiential observation of a business management process regarding risks during cloud migration. The purposeful sampling method provides prodigious information and will provide examples of information aligned with the research question of this study.

For this study, the selection of participants using a purposeful sampling method occurred. The ability of a participant to provide information valuable to the research question of this study was a necessity. The participant must have had direct knowledge of the risk management process used for the business's cloud migration. The participants must also have taken part in the cloud migration process at the business.

Similar to the population of this study, the choice of participants was not random. To research the management of risks encountered during cloud migration, the use of a purposeful sample was appropriate. The criteria described for the participants of this study was clear and discrete. The opportunity would exist for the exclusion of participants using a random sampling method. Purposive sampling using the described criteria ensured the participant sample met the needs of this study. Purposive sampling of the participants was appropriate for this study.

This study was a case study. The delimitation for the case study was that it includes no more than seven businesses. A gauge of saturation for this study occurred during the analysis of the participant interviews. When consistent duplication of information from the participants occurred, data saturation occurred. The participant interview information provided was reflective of each business in the population. The use of a purposive sampling method for the population enhanced the opportunity for data saturation. The use of purposive sampling also ensured the population meeting the delimitation of three businesses.

Data saturation was reviewed by analyzing the data of each new theme as it presented. A review of the data acquired from each of the participants of the population occurred weekly. When no new data points from the population existed, the population reached data saturation. The specific criteria required to be a participant in this study created a saturated sample pool. If a business in the population did not have sufficient participants, the selection of a new business occurred.

The researcher created a list of familiar businesses that met the study criteria. The determination of the list occurred when the population met the requirements of this study. Recruitment of the businesses through existing relationships of the researcher in the multiple industries occurred. Telephone discussions with senior leaders at each business to discuss the opportunity of this study took place. Upon confirmation the business accepted this study, the senior business representative provided a signed site consent letter.

Setting

The setting for this study was the location of business firms in the United States. The businesses were medium enterprises or larger defined in Gartner (2018). The size of the businesses ensured resources for interviews and the ability to reach data saturation for this study. Christensen et al. (2020) stated that the definition of a recruitment approach comes from the type of population needed for the study.

The population sample was purposive and deliberate, providing the best chance of success for this study. The recruitment process was fair and considerate, as well as ethical (Creswell & Poth, 2016). The selection of three businesses occurred. The basis for the selection of these businesses relied on the researcher's knowledge of the businesses and the associated cloud migration criteria. Advanced knowledge of each business depicting how the business met the requirements for this study saved time and eliminated exclusion.

The utilization of professional relationships occurred during the recruiting of each business. The researcher acted ethically by explaining the request for the study was an academic exercise and not for business purposes or profit. Each business leader received the presentation of this study proposal. Each business received provisions for inclusion in this study. The business decided to participate or not without regard to the prior relationship based on this study proposal.

Each business received an explanation of the interview process for this study. Each business had the discretion to provide an onsite location for the interviews. The use of an onsite location required a site permission document signed by a representative of the business. The use of an onsite location was not available for this study. The researcher provided alternate meeting arrangements. If a business allowed interviews to occur during work hours, the researcher

accommodated the use of work hours for the interviews. When a business would not allow interviews during work hours, each participant received an explanation of this requirement.

The use of industry information provided relevant criteria for the choice of businesses included in this study. Information collected from each business provided a result set relating to the case. The cumulative information from all of the results provided the triangulation of the data. The different vantage points from multiple businesses provide triangulation of the data (Carter, Bryant-Lukosius, DiCenso, Blythe & Neville 2014).

Merriam and Tisdell (2016) asserted that using case studies provides information that can be both specific and has generalizability. This case study accepted information from each business and provides scholars and practitioners the results of each business firm in aggregate. As a case study, this study will present results that can be generalized to different businesses with summative results.

For the academic, this study provides two types of results that do not exist now. The first type of result is a descriptive case study of the process of managing risks during cloud migration. The second type of result consists of aggregated information from multiple businesses describing risks during cloud migration. Academics will have the ability to use the results from this study for comparison purposes at either the aggregate or single business level.

The practitioner has a similar ability to the scholar to identify specific risk management processes from the results of each business case. The practitioner will also have the ability to view the results of this case study in aggregate. The generalized results will provide data previously unpublished regarding risk management processes utilized during cloud migration. Practitioners can use the aggregate results to prepopulate risk registers for cloud migration activities.

Analysis of the Research Questions

The research question for this study, how do large business firms in the United States manage the risks they encounter during the migration of cloud computing was one of management, of a technological change to the business. The precise manner of businesses managing risks during cloud migration will be studied. The process used to make decisions during cloud migrations happen. This study, when completed, will present the findings of the management process of risks during cloud migration.

Paying particular attention to the detailed and rich information collected as a part of the interviews will play an essential role in the analysis of the data. Christensen et al. (2020) asserted that inductive analysis and creative synthesis provide a superior approach for analysis of qualitative research. Schindler (2019) suggested that multiple standards of ethics exist. Further, the standards of the Belmont Report of 1979 and the Federal Register of 1991 must be adhered to as they are the impetus for modern research ethics (Schindler, 2019). The interview protocol for this study followed the Capella University code of ethics, as well as all federal, state, and local laws. The design protocols for the interviews of the participants were to protect the participants while allowing the interviewer the ability to capture the comprehensive information provided.

The protocol for the interviews includes five conventions. First, the recruitment of a prospective participant with an invitation to this study occurs. The invitation sent to the participant explains the interview process. The participant accepts or rejects the invitation and is accepted to participate in this study. Inclusion in this study includes a formal signature of the accompanied permission form. Second, during the initiation of the meeting, the participant was greeted and thanked for their participation. Third, the delivery of the research interview process occurs for each participant. Next, each participant must provide the researcher with any

questions if they do not understand the interview process or their rights of participation. The participant verbally affirmed their understanding and acceptance to participate in the interview and was recorded for transcription. Fourth, the interview begins with a series of questions related to gathering information about the research question of this study. Fifth, the participant was asked if they have anything else that they would like to provide to the interview. Finally, completion of the interview occurs, and the recording stopped. The participant was thanked again for their participation.

Credibility and Dependability

Creswell and Creswell (2018) asserted that key methods for founding credibility and dependability exist. Credibility is the primary and most important feature in qualitative research when establishing trust (Merriam & Tisdell, 2016). The credibility of this study comes from the use of different methods.

Researchers use the triangulation method to ensure the credibility of their study (Merriam & Tisdell, 2016). The construction of clear themes occurs from the collection of data from different sources (Creswell & Creswell, 2018). This study was a case study using businesses in the United States of America. Data collection came from multiple sources for this study. Data coming from different populations and participants within those populations provides credibility for this study. The capture of secondary instruments such as artifacts, documents, and transcripts described during the interview occurs to provide credibility to the statements in the interview from the participant.

Leedy and Ormrod (2018) asserted that validity and reliability are precise and persistent in the pattern, respectfully to the subject of study. Dependability and reliability in qualitative research are synonymous (Merriam & Tisdell, 2016). Dependability is almost as critical as

credibility in creating trustworthiness in research (Creswell & Creswell, 2018). The use of external peer review occurs as a part of this study. External peer review generated dependability and established trust.

A collection of data from different operational areas of each business transpired. The operational areas included the executive, IT management, and IT practitioner. The three areas in each business provided different vantage points of the same process. Leedy and Ormrod (2018) identified that researchers use a triangulation approach and collect different forms of data to identify and find persistent themes. Finally, during this study, the collection of different types of data occurred. Data from each of the businesses included interviews with participants and observational notes of the interviewer.

As a peer-review process, doctoral learners reviewed and evaluated this proposal, data analysis, and the data collected during this study. Each reviewer looked for bias, thick description, and counter thematic data. The peer-review included three areas. First, validation of data collected during the study occurred. Second, alignment between the data and the reported results were validated. Third, the evaluation of the study framework occurred. Finally, alignment between the research data and the research question utilizing the conceptual framework of this study occurred.

After each interview, the participants received a transcription of their interview. Allowance for each participant to read and provide corrections to the information occurred. Moreover, providing further credibility of this study, a member checking process occurred. When the completion of the data analysis of this study occurred, all participants receive a summary of the findings. A request for participant feedback from the results occurred after each participant received the results.

Finally, the researcher was reflective of the data collected. Each transcript was observed for personal bias and to verify bias against the transcripts from the interviews. A draft report was created for the final results and evaluated. Participants received the results of the draft report to validate for accuracy. The credibility and dependability of this study relied on multiple methods. Methods used in this study included triangulation, peer review, reflexivity, member checking, and participant accuracy checking. The combination of methods creates a credible and dependable study.

Data Collection

Six primary methods exist when collecting data for research (Christensen et al., 2020). Each of the six methods of data collection delivers optimal precision for the type of research associated with each method (Schindler, 2019). The use of an interview is the best way of capturing qualitative data (Christensen et al., 2020; Schindler, 2019). The use of an interview process for data collection for this qualitative descriptive case study occurred. First, the researcher introduced themselves to the participant. Next, an explanation of the interview processes with each participant occurred. The participant was set at ease through the explanation of the process and was allowed to ask questions. Next, each participant received an explanation of the details of this study. The participant then received a copy of the informed consent document. When the participant had no further questions, the participant signed the informed consent document and returned it. Completion of the preliminary interview process occurred when the informed consent document was signed and returned, and the interview began.

The interview process for this study consisted of three sets of interview questions. The first set of questions for this study served two purposes. First, the initial study questions asked the demographics of the participant. Second, the questions verify that the participant met the

criteria for inclusion in this study. The second set of questions was open-ended questions. The second set of questions populated the bulk of the thick descriptive results. The third and final set of questions had two types of questions. The first type of question was a structured question. The second type of question was a follow-up or probing question. Each probing question provided an opportunity to elicit more information from the participant.

Schindler (2019) asserted that the researcher defines the content in the research identifying participants, sampling, and acts, which are the areas coded. The coding structure for this study was structural design. Saldaña (2015) stated that structural coding processes entail conceptual phrases representing the questions of inquiry. The coding structure for this study evolved from the emerging themes and the processes identified. There were two rounds of coding. Moving from a gross level of coding to a more precise level of coding presented a clear view of the themes.

In qualitative research, interviews are common (Creswell & Creswell, 2018). Case studies rely on interviews to capture current and relevant events (Yin, 2014). This study was a qualitative case study. The primary instrument for data collection was the interviewer. As the interviewer, it was possible to create a potential bias that could cause the participant to answer the interview questions in a non-factual way. The demeanor the interviewer has should be polite and create a neutral environment in which the participant feels comfortable (Schindler, 2019).

Every effort to capture the factual data for this study occurred. All participants were asked questions in a polite and neutral tone. An atmosphere of professionalism and a level of trust between the researcher and the participant occurred. Using the interview method for research produced the best opportunity to capture accurate information based on the participant's responses to the interview questions. The researcher was attentive to all answers from the

participant. All participant answers to interview questions occurred truthfully and conscientiously.

Before the end of the interview, a query to each participant to provide more information occurred. The opportunity for each participant to ask final questions also occurred. The researcher provided answers to each question asked by participants. Each participant received appreciation for their participation in the study, and the interview ended.

Field Testing Interview Questions

Creswell and Creswell (2018) suggested that the testing of instruments provides clarity and the ability for improvement. This study was a qualitative study where the interviewer is the instrument collecting the information. The interviewer attempted to enhance his skills in interviewing using a preliminary field test of the interview questions for this study. The interviewer conducted a field test to check the flow of the interview as well as timing. An evaluation of the validity and clarity of this study's questions against the research question occurred. The researcher created all questions used within this study as well as subsequent revisions of any questions. The completion of a field test of the interview process following the interview protocol occurred. Each test participant met the participant criteria for this study. However, the inclusion of the organizations the test participants were employed by did not occur in this study. The inclusion of the test participants also did not occur in this study.

Before the actual collection of research data for this study, a field test of the study questions for the interviews occurred. The participants for the field test came from working relationships with the researcher. The constraints of the test limited initial feedback to three participants. A participant from each of the three areas outlined in Chapter 3, design, and methodology was selected to participate. The participants included executive management, IT

management, and IT practitioners. Each of the field test participants was asked questions from the research study questions.

All participants selected for the field test met the original criteria outlined above in the design section of Chapter 3. All of the participants have worked for businesses that have migrated to cloud computing within the past five years. Additionally, each participant had direct knowledge and participation in the adoption and ultimate migration of their respective organization's data to the cloud. Each of the identified participants agreed to partake in a trial interview with the researcher.

The inclusion of the following participant areas of the field test occurred, a business level executive with direct input regarding governance for her organization, an IT managerial level facilitator, and an IT practitioner. The resultant interviews ranged in time from 28 to 51 minutes from start to finish, including the explanation of the informed consent. There was no recording of the test interviews. All questions functioned and resulted in answers of various length and description. The next steps post scientific merit review would be initial data gathering from the first set of actual research participants.

Data Collection Process

The data collection process for this qualitative research study includes phases. The initial recruitment phase included the researcher engaging with the business, providing the participant criteria to the respective department within the business that provided the researcher with the ability to conduct the research. Next, on behalf of the researcher, authorized representatives from an employee resource department initiated the first contact between the identified employee participant and the researcher by providing contact information of the researcher to the employee. Contacting the participants in this manner enabled privacy from the beginning of the

process as well as instilling a level of trust by conducting initial contact with the business's internal employee resources representative.

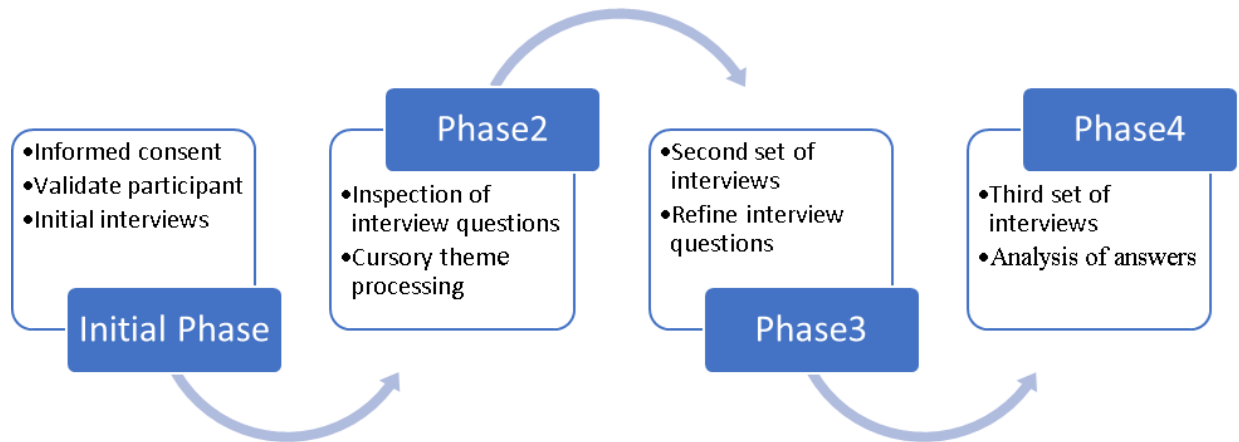


Figure 4. Data collection flow chart.

Four total phases completed the data collection process for this study, as identified in Figure 4. The phases consisted of (a) confirmation and validation of the contributor along with initial interviews; (b) identification of themes based on initial interviews; (c) a second set of interviews; (d) the third set of interviews; and (e) the final and fourth set of interviews. The process was iterative, which provided for the refinement of the interview questions to better align them with the research question. Schindler (2019) asserts the participant will be more at ease when accommodations to their contribution occur. The interview process consisted of the researcher and the participant conversing using the Zoom conferencing software. The meetings occurred through the Zoom conferencing software at a time that was best suited to the participant.

The interaction was a question and response format. The process started with the researcher asking question one proceeding to the end of the questions, or until the employee was no longer willing to participate. Another opportunity to complete the interview was available if a

participant departs the interview early. If this was not possible or the employee denies the opportunity, entry of the completed questions to that point occurs in the pool of existing answers for this study. Each interview operated the same, with the addition of previous answers to the questions supplied after the respondent has offered their reply, offering the contributor the ability to supplement the offered answer.

Initiation phase. The initial phase began with the researcher producing the documentation for this study once approved by the authorized executive representative of the business. Leedy and Ormrod (2018) suggested that the documents for the interaction between the reviewer and the population and participants provided to provide clear information. The initial documents included (a) formal criteria for employee inclusion in this study, (b) documentation to be provided to the contributing employees, (c) contact information of the researcher, (d) request to schedule an appointment for an interview, (e) a sample informed consent form, and (f) documentation of the risks and benefits of this study. Next, the employee resources department made the first contact with the eligible employees for this study, providing each employee with a set of documents given to the department by the researcher. When a participant contacted the researcher, the following steps occurred. The use of criteria for this study to validate the participant occurred. The participants scheduled the time of the interview with the interviewer. The researcher answered all of the questions the employee had about this study.

Step 1. Creswell and Poth (2016) assert that ethically participants must know their participation rights in research studies. The initial phase of the interview process includes the researcher providing the participant with the informed consent document. Next, the researcher explains the risks and benefits of this study. The participant receives the document the

researcher then explains the risks and benefits to the employee as well as answering all questions the employee may have about this study. Next, the researcher proceeds to capture the responses to the interview questions from the participant.

Step 2. Interviews from the first business occur. An interview with each qualified participant occurred. When and where possible, the collection of artifacts provided by the business occurs.

Step 3. Interviews with successive businesses occurred. The order of interviews for employees occurs with the availability of the participants. The collection of artifacts provided by the business relating to the research question occurs.

Step 4. The final step in the data collection was interviews with the employees of the third business. The final interviews collected from the third business takes place. As with the previous interviews, the collection of provided artifacts relating to the research question occurs.

Data Analysis

Research data analysis of open-ended qualitative questions can be quite laborious (Christensen et al., 2020). The design of interview questions should be logical and related to the research question (Leedy & Ormrod, 2018). This study was a qualitative case study based on the experience of the participants. The data collected for this study came in three formats. First, operational documents describing the process the businesses used during the cloud migration. Second, the creation of transcripts from the interview and interviewer's notes happen. Finally, with the permission of each participant, an audio record of the interview using computer software occurred. The exclusion of a participant occurred if they did not grant permission for a recording of the interview. The interviewer records the interview and nonverbal cues as well as other attributes through the course of the interview. The electronic method was the preferred

method to capture the interview. The use of Zoom software to capture the audio portion of the interviews provided accuracy. Through the reading of the transcription, the accuracy of the interview occurred.

The notes taken by the interviewer of the nonverbal cues and body language included different qualities. The interview notes included the tone of the voice, the speed of the answer, pauses, gestures, facial expressions, and body movements as a part of the interviewer notes. These nonverbal responses provided insight into the way the participant responded to each question. A record of changes that occur during the interview occurs. The capture of possible themes from the interview transpires. A record of the non-verbal responses occurs with questions through post-interview transcription and evaluation. Each participant received a transcription of their interview, and validation of their agreement ended. Interview notes and electronic audio recordings are the most ethical and best choice for case studies with interviews.

The collection of documents provided by the business, including risk registers, Gantt charts, project plans, task assignments, and monetary or resource allocation artifacts, occurs. Any documents provided by the businesses are in electronic format only. Utilizing an electronic format for documents reduces the accidental loss of work products from the businesses. The business has the discretion to provide storage of electronic documents. The interviewer offered a secure, encrypted, and password-protected media that prevented unauthorized access to the data. Utilizing a document collection method using high encryption was the best for this study, providing protection of the documents for the businesses as well as ease of transfer to this study repository.

The conceptual framework for this study was adapted using the stages of design thinking. The use of the conceptual framework for this study to categorize and code the emerging themes

was employed. The five stages of design thinking, including empathy, definition, ideate, prototype, and test deliver lenses through which a framework was built (Mickahail, 2015). The conceptual framework areas align with the emerging themes of this study. Each stage of the conceptual framework of this study was unique.

The creation of a repository using the NVivo version 12 software occurred. The initiation of the transcription process began. The process consisted of data analysis through the creation of a single repository for all data segments collected. All transcribed information resided in the NVivo repository for the duration of this study. Next, the transcribing and notating of all collected documents occurred. The data entered into the NVivo software became searchable. Next, the loading of the transcriptions and the operational notes taken by the researcher into the repository occurred. Finally, the loading of all remaining transcriptions along with the notes taken during the interviews into the repository occurred.

The next portion of the analysis has two activities: data loading and remediation activity. Identification of data errors and anomalies in the data occurred. Observation of issues causes the removal of errant data, broken or misplaced information, misaligned segments of data, and other anomalies to another location for remediation, including observation and possible reintegration, occurs. Data cleaning was a regular operation of research and analysis, including the removal of errant or missing data as well as data not aligned to the study (Graziotin, Fagerholm, Wang, & Abrahamsson, 2018).

I validated the remaining data for misspelled words, broken or truncated words or objects, alignment, and syntax, and other common deficiencies that occurred during the transcription processes. Once the data validation was complete, the processing of removed data a second time for possible inclusion occurred. Data found viable was added back to the

repository. Once all the documents, interviews, and operational and other notes have been transcribed and coalesced into a working repository, the data analysis process began. Next, cleansing of the data of formatting and errant issues occurred. The use of NVivo version 12 software for a second effort to evaluate and analyze the cleaned data for qualitative analysis and reporting occurred.

The use of NVivo version 12 software for the data analysis occurred. The use of the NVivo version 12 software develops structures and finds significant themes within the data collected for this study. The coding of content using standard codes for case studies such as attribute, descriptive, dramaturgical, emotion, holistic, In Vivo, narrative, process, versus aligned to the types of textual data (Saldaña, 2015).

The basis for coding each document considers the scheme of the categories and attributes of the data from each responding business participant. Saldaña (2015) asserted the application of different levels of coding at different points in the findings of research occurs. The data from each of the three businesses have unique coding identifying the originator of the data. The coding of data using multiple levels to identify the distinct themes and content of the data for this study occurred. The capture of word frequency, themes, and other categories from the interview data using the NVivo version 12 software occurred.

Battleson et al. (2016) asserted that the interviews conducted for his study included participants who had been through the cloud migration or were currently going through cloud migration activities. Battleson et al. stated that the duration of the interview was approximately one hour in duration. The field test of the interview questions for this study provided results that approximated one hour of duration for a test interview. The amount of time estimated for each face-to-face interview was one hour. If the interview exceeds one hour, a reassessment of the

interview questions occurs. Previous research conducted on cloud computing provided similar timelines for demonstrating the expected time with participants for this study was accurate.

Christensen et al. (2020) suggested that triangulation of themes in well coded and categorized data is present in research studies. A demonstration of triangulation for this study uses the sources from different businesses by presenting multiple data points. The identification of significant themes was determined when data saturation happens. When data saturation occurs, the capture of information from the interviews for this study ends.

The findings of this study present a thick description of the interview with each business. The format is a textual list of significant themes, sentiments, and attributes found in the data. A presentation of tabular data, including the common themes and shared traits exists. One table has a column list of the cloud migration and the management process used for risks encountered during cloud migration, where the rows contain the qualitative data provided by the participants from the interviews. Table 1 is an example of theme data from this study. The data is available to be viewed in its raw format as well as represented in different visual formats. Visualization of data through tabulation and graphic representations of themes provides one presentation method.

Table 1

Cloud Migration Data Collection Example

Risk	Category	Level	Management Process
Unauthorized Access	Security	Low	Remediate using multi-factor authentication
Data Security	Security	High	Protect data using encryption

Visual analysis of data for common patterns and associations is visible in graphical formats (Saldaña, 2015). The graphical representations are a fast way to view and analyze data. Data visualizations, including bar charts, pie charts, and plot graphs, are types of visualizations that help researchers observe data. Presentations of data for this study are qualitative and not statistical. This study presents data using a bar graph with the percentages of the most common themes. Finally, a report describing the analysis of the themes of this study occurred.

Ethical Considerations

Many considerations are involved in formal research. The most important considerations include the ethical considerations a researcher must undertake in gathering information from humans (Christensen et al., 2020). This study meets the ethical standards for research. This study includes observance of the following: (a) no harm in a physical or psychological manifestation came to a participant; (b) during this study or post-publication of this study's findings no harm occurred to the business; (c) there are no monetary considerations that are burdensome for either the business or the participants of this study; and (d) informed consent was needed from the participants of this study including the business. Christensen et al. (2020) suggested that the transaction of research provides no detrimental actions to the subjects of that research.

For this study, adherence to the three principles provided in the *Belmont Report* of 1979 concerning the treatment of human subjects, including respect for persons, beneficence, and justice, was followed (U.S. Department of Health and Human Services, 1979). To that end, all participants were treated with respect before, during, and after the interview process. All measures needed to provide a positive outcome for the participants of this study occurred. Participants of this study received equal, equitable, and fair treatment as well as consideration throughout the process of this study.

Schindler (2019) suggested acquiring the cooperation of the business and support of the leader of the business is requisite for a study. As a prerequisite of this case study, permission from the chief business leader, allowing the involvement of all prospective employees, was a requirement. Schindler asserted a signed consent from each employee participant is required. All participants are required to sign a consent for this study.

This study, by its nature, captures actual risks encountered by the business during cloud migration and implementation. The interview and data collection phase of this study might capture data that a participant could perceive as harmful. Christensen et al. (2020) described areas of data collection that participants might interpret as harmful either to themselves or the organization to which they belong. The participants of this study could perceive an ethical issue as harmful.

Christensen et al. (2020) stated that researchers have an obligation to the population and participants to do no harm. The researcher's duty to the business and participants of this study created a state of nonmaleficence. During the research collection of this study, the researcher protected the interests of the population and the participants. The researcher continues to protect

the population and the participants of this study in perpetuity. The researcher operated using ethical standards about all research studies.

Christensen et al. (2020) asserted the information collected by the researcher be coded and obfuscated in a way that would protect the population and participants of this study. This study used a coding scheme for the data collected. The coding scheme provided an alignment between the respondents and their answers. Using this coding scheme generated obfuscation of the results that masked the data and preserved anonymity.

To best serve both parties, the raw data was further be anonymized. Data aggregation occurred as well as the consolidation of emerging themes. The individual responses were anonymized and redacted. Cleaning the data prevents all subsequent searches from identifying the source of the collected information. The collected data was masked and presented in aggregate. Anonymization of these parts of the findings of this study prevents the identification of the participants and the businesses.

The period for safeguarding the data does not exceed seven years past the publication date of this study. The storage of all artifacts until their destruction is the researcher's responsibility. The researcher takes every precaution to prevent unauthorized access to the collected data. Physical safeguards include locking the storage device of the collected data when not in active use. The storage of other artifacts is in the same locking storage device used to store the encrypted data when not in active use.

Until the time of the destruction of the data for this study, all collected data is software encrypted using 2048-Bit encryption. Before publication, the storage of collected data exists on software devices at the researcher's primary domicile. The data collected is not to be stored in a

cloud or central network storage area such as Google, AWS, or Azure. The destruction of all soft-copies of data not ready for publication occurred following DoD standards.

The collected data is secured using a complex password. The creation of the password includes using a random password generator. The password criteria include length, complexity, case sensitivity, special characters, and numeric characters. The requirement of password protection of the data involves the following parameters. The password length is no less than 20 characters. Password complexity includes upper and lower case letters. At least one numerical value and one special character must be present within the password. The location of the password exists outside of the internet.

The movement of all files of this study occurs upon publication of this research study. The storage of data exists on a physical device with hardware-based 256-bit AES encryption. Availability is allowed to the researcher and the researcher's committee chair for the seven years of retention. The device is located and secured in a safe at the researcher's primary domicile.

Destruction of the collected data occurs after the publication of this research study. Seven years after the publication of this research study, the destruction of the data will occur. The process for destruction of the data will follow the Department of Defense (DoD) standards and methods. The DoD standards include "Methods used for clearing, sanitization or destruction of classified IT equipment and media include overwriting, degaussing, sanding, and physical destruction of components or media" (Department of Defense [DoD], 2013, pp. 42-44).

CHAPTER 4. RESULTS

Introduction

This fourth chapter presents the research aspects and the qualitative analysis of this study. A presentation of the results of this study exists in two parts. Part one presents the research findings collected by the researcher. Part two presents a qualitative analysis of the research.

Creswell and Poth (2016), assert that the interviewer of a research study is the instrument for that study. The instrument for this study was the principal investigator. The importance of identifying the researcher as the data capture point reveals the opportunity for bias. The experience of the investigator provides the opportunity for bias and can create issues with the validity of the research. Understanding the possibility of bias provides the opportunity to ease attitudes and other contentious information extracted from the participants and subsequent interviews.

Creswell and Poth (2016), suggest that interviews for a qualitative gathering of research provide reliable information when shadowing the participant is not possible, particularly in the case of past events. This study does not use qualitative instruments, such as surveys. The research intent was to gather a raw set of information with minimal bias. Analysis of the collection for emergent themes arising in the interviews progressed. Each query posed to the population for this study advanced through multiple development iterations. Four iterations of questions occurred before the final questions used for this research. The outcome was inquiries with the least amount of bias introduced through the question.

Qualitative studies can utilize many forms of data collection, including personal interviews or surveys (Saldaña, 2015). The data collected for this study comes from semi-structured interviews of participants. The interviews occurred via computer teleconference using Zoom software. The recordings of the interviews included only the audio portion. Each participant provided permission for recording the audio of the interview. The audio recordings were captured and stored locally. Immediately following the interview, relocation of the recorded files to a non-internet connected computer for security occurred. The audio recordings were then transcribed and stored on the same non-internet connected computer.

Working as a technology consultant, the researcher was familiar with and had viewed a proliferation of businesses migrating to cloud computing. The choice of research for this study was the researcher's area of work endeavor. A large number of migrations to cloud computing piqued an interest in understanding the complexity of this task. The researcher's prior experience with both cloud computing as well as management and business continuity provide a depth and ability to complete this research study.

Data Collection Results

The methodology employed to collect the information for this study was a descriptive qualitative case study. There are two noteworthy design characteristics for this study. First, using purposeful sampling to identify and collect data. The second design characteristic was the analysis framework. Christensen et al. (2020) suggested that the discovery of thematic commonalities can arise using inductive analysis and creative synthesis. The application of metasummary as a process can detect themes across multiple sources using inductive analysis (Saldaña, 2015). As an example, a comparison of the responses from business executives from

multiple organizations can provide shared elements. The analysis framework used the inductive analysis along with creative synthesis on the data to provide the results for this study.

The purpose of this study was to add to the body of knowledge concerning cloud migrations and the management processes used for risks during those migrations. Using interviews to capture information from participants with descriptive information provides rich and thick details (Creswell & Poth, 2016). The collection of interview data provided information about the migration to cloud computing and the risks associated with the migration. There existed no alternate way to gather complete information from businesses regarding cloud migrations. A single observer would have to have occurred in each business at all levels of the business to collect the same information. The data collected in this research demonstrated that the collection method for this case study was ideal.

Research Population Identification

It is the responsibility of the researcher to target the population for the study (Schindler, 2019). Identifying a population for this study was not difficult. Each research population has characteristics and parameters that describe its various features (Christensen et al., 2020). The population came from businesses in the United States. The parameters for the population included a cloud migration within the past five years, and income higher than \$50B annually.

Research Population Recruitment

Recruiting the population for this research study was long and not without pain points. Saldaña (2015) asserted that it could be hard to recruit desirable participants. The recruitment of businesses for this study was difficult. Contact with multiple businesses in the United States occurred. The first 37 businesses offered no consideration for this research study and declined to participate.

Commonalities between the businesses contacted that were unwilling to participate included no professional relationship with the researcher. In other words, cold calling businesses for research failed. Based on this identified defect in recruiting a research population, a new attempt was necessary. Maramwidze-Merrison (2016) suggested removing the difficulties in the acquisition of populations through contact on a professional level. Maramwidze-Merrison further defined ways using the researcher's professional network of contacts. The next attempt included recruiting a population through contacting businesses where a professional relationship existed with employees.

Successful recruitment of five business occurred. The submission of a formal recruitment letter to each business occurred that included the requirements of this study and Federal legal information for research to each business. However, the complete study of only three businesses occurred. Two of the businesses that responded positively withdrew consideration to participate in this study. Information collected from the businesses before the withdrawal from consideration was included anecdotally within the aggregate data.

A complete study of each of the remaining three businesses that accepted the request and returned the consenting paperwork occurred. An open dialogue between the researcher and senior leadership within each of the businesses occurred. The alignment of the population, participants, and events to be studied, created a purposeful sampling depicted in Chapter 3. Maramwidze-Merrison (2016) identified that by providing prospective recruits with information regarding the value of their participation would create an investment on their part. Contact with a second business occurred where a professional relationship existed with the researcher during the same period as the first business. Two weeks following the first study acceptance, the other business provided authorization to conduct research. The same method of contacting the

executive sponsor at each business and providing an explanation of the criteria for the study participants occurred. Presentation of a list of possible participants as well as permission to use internal email addresses for recruitment occurred.

Of the five businesses providing acceptance of this research study, only three completed the entire study. The final population consisted of three businesses in the United States. Each business was in a different industry. All of the businesses met the requirements for inclusion in this study, including the revenue, size, location criteria.

The type of cloud migrations discussed regarding risks was of two types. The first type of migration consisted of infrastructure as a service (IaaS). The second type of migration was software as a service (SaaS). All businesses provided information concerning risk management for cloud migration to either an IaaS or SaaS migration.

Research Participants

Recruitment of the participants followed the recruitment of the population of each business. Leedy and Ormrod (2018) asserted that making research enjoyable provides better opportunities to recruit participants. A two-step process to recruit participants occurred. First, each business accepted the research study and provided the participant's email addresses. Second, recruited participants received clear and concise recruitment emails explaining the research study and the participant's eligibility to participate. The recruitment letter was purposeful in the explanation of the participant's rights not to participate as well. Each business had possible participants identified that chose not to respond.

This study included participants from three areas of operations within each business, as outlined in Chapter 3, including executive business management, IT management, and IT practitioners. Alignment with the participants and the research question occurred. Recruiting

the participants from the three areas within each business demonstrated the alignment between the research question and the population. The participants from these three areas provided useful information and the ability to triangulate the data from three separate orientations in the business related to the same events. The total number of participants for this study was 11. The final number of fully qualified participants was five, demonstrated in Table 2.

Table 2

Participant Demographics Detail

Employee	Job Title	Tenure (years)	Functional Area	Participation Type
Employee 1	IT Manager	8	IT Management	Full
Employee 2	VP Business Operations	38	Business Executive	Full
Employee 3	CIO	14	Senior IT Management	Full
Employee 4	IT Director	10	IT Practitioner	Full
Employee 5	COO	4	Business Executive	Full
Employee 6	CIO	6	Senior IT Management	Partial
Employee 7	IT Director	5	IT Practitioner	Partial
Employee 8	CIO	4	Senior IT Management	Partial
Employee 9	Enterprise Architect	3	IT Practitioner	Partial
Employee 10	CEO	25	Business Executive	Partial
Employee 11	COO	22	Business Executive	Partial

Each participant received delivery of the criteria for this study as a part of the recruitment. A presentation of the provisions of the criteria and an explanation of each occurred. Maramwidze-Merrison (2016) suggested that participants understand possible outcomes of research and the part the participant played, making contributions easier to attain. Each participating business provided internal email addresses with permission to use them for

recruitment for this research study. The arrangement for identification and contacting participants occurred during the dialogue with business executives. The use of this recruiting method proved fruitful for each new business going forward.

Each participant interview delivered a different point of view concerning the way risks were observed and managed. Collecting information for this study was an aggregation of experience from business and information technology professionals. Each participant was contacted and asked to participate in this study with the researcher's knowledge of the participant's experience with cloud migration at their respective business. The participants came from different roles within the business and their experiential knowledge of cloud migration.

Schindler (2019) suggested that participants completing a partial scenario encouraged details not typically discovered through other means. The interview process was self-explanatory. Each interview used open-ended questions that allowed for elaboration from the participants. Follow-up and probative questions followed the open-ended interview questions to provide a closer alignment to the research question. Using scenarios allowed the participants to provide information on their cloud migration.

Each interview consisted of a computer video conference using Zoom software. A recording of the audio portion of each interview took place. Recording each interview met academic requirements. The transcription of each interview occurred from the corresponding audio recording. The combination of the transcription and the audio recording increased the validity and analysis of each interview to occur. It further allowed the researcher to send the transcription to each of the participants to validate for errors and corrections.

There were multiple logistics involved with the interview process, including the timing related to both scheduled interviews and the timeframe of the interview itself. The interview

scheduling process, while not cumbersome, was a challenge. The timeline for scheduling the interview and performing the interview was one week. Each interview included a buffer. The added time between each interview prevented overlap with other participants. Participants received notice of the time frame for the interview. The only limitation for the time was the participant's responses. Each participant was allowed as much time as they wanted to respond to each question. The interview process, including the video conference, was 45 minutes to one hour in length. The shortest interview was 38 minutes, with the longest taking 65 minutes.

The interview questions consisted of four sections. The first section included the demographics, agreement to participate in this study, and the participant's qualifications to verify they met the criteria for this study. The second section had questions used to identify the events related to the research question process management of risks during migration to cloud computing. The second set of questions was to establish a baseline of information before cloud migration. The third set of questions was asked of the participant to describe the process during the migration. The fourth and final section included questions asked of the participant to determine mitigation and process post-migration to the cloud as well as a final question if the participant wanted to add any other information that might be pertinent to this study.

The interviews of the study participants followed the five interview protocol conventions outlined in Chapter 3. Each possible participant received the initial recruitment letter through internal email at their business. A second email provided the participant with the informed consent form. Each study participant accepted and returned the permission form. Next, the interview was scheduled as soon as possible within the dates provided by the participant.

Creswell and Creswell (2018) asserted that the researcher collects data from structured or semi-structured conversations. Each Zoom conference with the study participants was a semi-

structured interview. After appreciation for participating in the study occurred, the participants received information about the interview process was explained, followed by the participant's rights of participation. Following the explanation of the participant's rights, a verbal acceptance and acknowledgment of the interview process by the participant occurred.

Next, the interview began introductions ensued. Each participant provided demographic information to the interviewer. The participant responded to 12 questions. The interview questions were open-ended to provide the participant with the opportunity to respond with as much rich detail as they chose to.

Data Analysis and Results

The second section of Chapter 4 presents the results and analysis of the data collected. All data collected for this study was anonymized. Anonymizing the data protects the participants and the businesses they represented during the interviews. The anonymizing of data was done through coding, as well as presenting the results was an aggregate format. Using these two methods creates successful obfuscation and data anonymization protecting both the participants and the businesses which they are representing. Finally, a presentation of the summarized data results with the identification of the key findings occurs.

Rahman et al. (2017) asserted that it is possible to predict a risk when governance exists to mitigate the risk. The interviews provided insight into the three different businesses providing information regarding risk mitigation. There was no register of risks either possible, existent for any of the cloud migrations discussed. The idea of creating a process to mitigate possible issues did not exist for any of the three businesses.

Islam et al. (2017) asserted that gross defects in cloud migration are possible when businesses are not prepared to manage risks. The responses from the study population about risk

mitigation and management process were nearly identical. The preparation of a management framework or other formal risk disposition process did not exist until after an issue was encountered. No participants described a framework to handle “what if” scenarios as a part of the planning for cloud migration. All interview responses asserted a reactionary response.

Aggregated Results

The following is a presentation of the semi-structured interview results, including the summarized answers provided by the participants. The interview questions cover three areas. The first set of interview questions references the period before cloud migration. The first set of interview questions pertains to processes and activities before migration to the cloud. The second set of interview questions pertains to the management of risks during the cloud migration. The final set of interview questions pertains to the actions the business took when risk was realized and became an adverse issue to the business.

Interview Question 1. Can you provide the date of the migration? The first interview question asked of the participants concerned the timeframe of the cloud migration. Question one identified the theme of duration. Three identifying codes to identify the duration from the participant responses exist, including short, moderate, and extended. The timeframe of a cloud migration provides the scope and level of effort a business uses to accomplish the migration tasks. The participant’s responses to the question ranged from 1 month to 34 months. Table 3 presents the different timelines for each cloud migration.

The cloud migrations discussed in the interviews provided three periods of duration. The duration periods included short, moderate, and extended. The first duration period identified existed at less than three months and was a short migration. The next group of migrations was longer than three months but less than 12 months identified as moderate migrations. The last

group of migrations included a duration longer than two years and classified as extended duration.

The complexity of the migration defined the durations. The implementation of the short migration occurred solely by the internal IT group of the organization. One of the moderate cloud migrations was completed by an internal IT group, while management of the second moderate migration occurred by both the internal IT group and an external vendor. Finally, the two extended migrations were handled exclusively by external vendors with the internal IT groups providing vendor management and oversight.

Table 3

Cloud Migration Detail

System	Business Function	Length (in months)
CRM	Operations	10
ERP	Operations	24
Communication	Email	8
Backup	Continuity	1
ERP	Operations	34

Interview Question 2. Was there a name for this migration or project? The second interview question asked of the participants provided the opportunity to validate an alignment between the business and the IT group by identifying the name of the cloud migration.

Generalizing the name of the migration provides internal identification as well as identifying the function of the migration. The participants responded with minor variations but aligned with a consensus of the actual goal of the cloud migration.

Only one migration existed without a formal identity, and it was an internal IT infrastructure migration. The name of the remaining migrations aligned with the business system in which they were associated. The migration identities included were ERP, CRM, and email. There were five different cloud migrations. Each cloud migration consisted of critical systems for the business. The types of migrations and locations, as well as the duration of the migrations, are demonstrated in Table 4.

Table 4

Cloud Migration Platform Type

System	Cloud Platform
CRM	SaaS
ERP	SaaS
Communication	SaaS
Backup	IaaS
ERP	SaaS

Interview Question 3. (Pre-cloud migration) Were there meetings to manage the risks?

The third interview question presented to each participant asked about specific meetings to discuss risks associated with cloud migration before the migration. The question queried if risk meetings took place and who attended the meetings? Each participant responded similarly, stating that the discussion of risks did not occur in a dedicated meeting. The discussion of risks occurred in other operational or business meetings.

Next, the presentation of a follow-up question occurred with each participant. The probing question was to determine the audience of the meetings where discussion of risks did occur. There existed further consensus amongst participants stating there were two categories of

meetings. The first type of meeting was a general business meeting to discuss multiple topics. The second meeting type was specific to IT related topics.

All participants responded that the business team only attended the general business meetings. Only the IT group was in attendance at the IT-specific meeting at each business. The IT group also attended the general business meetings where discussion of risks occurred.

The participants responded that members of the business operations and administration participated in meetings. The participants further noted that at least one IT member and one IT manager attended business meetings. The participants further detailed that a project manager attended a majority of meetings when the discussion of risks occurred. A notable absence of the migration sponsors existed regarding attendance of either type of meeting where the discussion of risks happened.

Interview Question 4. (Pre-cloud migration) What was your role in risk management at your organization before cloud migration? The intent of the interview question four intended to provide information that could be correlated to interview question eight. The combination of questions four and eight provide data relating to risk management processes.

Questions four and eight are nearly identical, but period centric. Question four queries the risk processes before cloud migration, while question eight examines the risk process after the migration has begun. Again each set of responses was in alignment with the participant's function in the business. Interview question four elicited two different responses from the participants.

The first set of responses fall under the IT group. All IT group participants identified themselves as responsible for managing technical risks. The IT participants expanded their responses to their group describing a direct responsibility for managing all technical risks

relating to the information technology functions of the business. Each participant qualified this response from the IT participants to only the technical risks.

The second set of responses was from the business participants. The business participants each asserted their role in risk management was not a direct role. The non-technical business participants described their risk management role as observation and dissemination of information to the leaders managing the migration. These business participants elaborated, further describing the information provided was at a high level. The business participants further described the leaders of the migrations as external vendors or project managers. This identification of the migration leaders removes the IT group as leading the migrations.

Interview Question 5. What did your firm do to identify risks associated with the cloud migration specifically, and did your firm use the same process before the migration to manage risks of the cloud migration? If the process was different, what changed? Question five presented the participants with the opportunity to explain the steps taken to identify risks with cloud migration.

The business participants provided answers relating to exploring information from vendors relating to the aspects of the migration. The business participants relied on information provided from external sources to the business. The IT group, both at a senior management level and the practitioner level responded similarly. The IT group responses asserted that they researched industry articles, spoke with external vendors, as well as speaking to peers in other organizations who had already migrated to cloud computing.

There was continuity between business participants and IT participants regarding a preliminary study. Participants from both the business and IT groups described a proof of concept (POC) exercise. The POC happened before the actual migration to the cloud. The

identification of risks and issues occurred during this POC exercise. However, there was no prescribed attention paid to the results of the POC regarding risks. The results of POC went without further attention.

Interview Question 6. What role did you play in the management of risks during the migration to cloud computing? Question six provided an opportunity for the participant to discuss their role in identifying risk occurrence during cloud migration.

A separation of the answers the participant has provided aligned with roles in the business. Participants working in the business at executive roles outside of technology described their role as active observers. The business executives indicated they did not actively participate in managing risks. Further elaboration from the business executives described the leaders of the migration managing risks. The participant's description included both internal business employees and external vendors.

The IT group participants asserted that they were directly involved with risk management. Again the IT group qualified the risks they were managing as technical only in their scope. Working with business users and external vendors during the migration, the IT participants described the management of risks. The nature of the information provided by the participants frequently described issues rather than risks. It became apparent that the management was focusing on issues.

Interview Question 7. Were there meetings to manage the risks of cloud migration, and if so, who attended the risk management meetings? Question seven presented the participants with a question about the business and risk management processes. The purpose of the question was to identify if meetings to discuss risks associated with cloud migration during the migration occurred.

All participants responded that they did not recall meetings with an exclusive purpose of risk management. All participants did respond that meetings occurred where the discussion of risks was a topic. There were variations between participant's responses to the frequency and the attendance of the meetings with discussions of risks. The frequency of meetings discussing risks in the enterprise had an occurrence between one per week to as infrequent as a few times per year, as demonstrated in Table 5. Meetings where the discussion of risks occurred also varied. All meetings described having the IT group in attendance, with various members of the business departments attending at differing times.

Table 5

Risk Meeting Detail

Cloud Migration (by company)	Meeting Category	Meeting Frequency	Meeting Attendees
1	Business Operation	Weekly	IT Group, Executive Management, Business Operations
1	Information Technology	Weekly	IT Group
2	Information Technology	Weekly	IT Group
3	Information Technology	Quarterly	IT Group
4	Information Technology	Weekly	IT Group
5	Project Management	Bi-weekly	IT Group, Project Management, Business Operations

Interview Question 8. What role did you play in the management of risks during the migration to cloud computing, and did you identify risks during the migration to cloud

computing? Question eight explored the actual events of the business during the cloud migration regarding risks. Question eight, similar to question four, measures the risk identification, through the cloud migration process and not before it.

Together the business participants and the IT participants responded with a consensus. All participants described the actions that occurred to mitigate the risks when they became issues during the cloud migration? The participant descriptions provided the identification of each risk as an issue occurred.

The participants described the mitigation process as having the three steps. First, research of the issue identified occurred for previous instances of existence. The outcome of the research determined the next steps of mitigating the issue. If the research provided a previous instance of the issue and a solution existed which resolved it, the existing solution was applied by the IT group immediately; if the research failed to provide an example of the issue with a solution, a new solution was created and applied immediately by the IT group.

The participants did not elaborate on the research method or location. The participants provided no specific actions taken. The participants only described a general outline of the process to mitigate adverse issues. The prevailing descriptions explained that if an adverse issue was found and identified that the IT group mitigated it immediately. Table 6 demonstrates the risk and issue management outlined by the participants.

Table 6

Risk Management Process Detail

Risk Management Process	Business 1	Business 2	Business 3
Formal Risk Process	No	No	No
Risk Process Meetings	Indirect	Indirect	Direct
Meeting Minutes with Action Items	No	Yes	Yes
Risk Identification	Indirect	Indirect	Direct
Risk Mitigation Management	IT Group/Vendors	IT Group	IT Group/Vendors
Risk Mitigation Action	IT Group/Vendors	IT Group	IT Group/Vendors
Risk knowledgebase created	Yes	No	No

Interview Question 9. Who was responsible for the management of adverse events for your firm during the migration to cloud computing? The ninth question explored with the participants and queried who managed the risks discovered during the cloud migration. The participant answers were similar and aligned between the business participants and the IT group participants.

The business participants asserted that the project managers, IT groups, and external vendors managed the risks during the cloud migration. Statements of external vendors partially align with the IT group participant's responses. The IT group participants asserted that they managed the risks as well as mitigated a risk that became an actual issue. In Table 7, a demonstration of the variance of the risk responsibilities by each company exists.

Table 7

Risk Management Responsibilities

Cloud Migration (by company)	Migration Type	Risk Identification	Risk Management
1	SaaS	IT Group/Vendor	Vendor
2	SaaS	IT Group	Vendor
3	IaaS	IT Group	Vendor
4	SaaS	IT Group/Vendor	Vendor

Interview Question 10. Was a knowledge base or other area of notes taken on the management of adverse events during the migration to cloud computing? Question 10 was to determine if the creation of a knowledge base containing risks and associated mitigation methods for cloud migration occurred. A majority of the participants initially suggested that inclusion of the risk information occurred in the project documentation as part of a status given in the various meetings. However, the participants were unable to provide any of the meeting documentation with status information.

All participants suggested that only the casual collection of information concerning risks occurred. Participants were unable to identify a formal place or registry where any documentation existed regarding risks or issues of the cloud migration. The participants' further elaborated that the creation of informal documentation occurred at the time the issue existed. The participant responses suggested that the documentation did not exist beyond the mitigation of the issue. The participant responses precluded the creation of a knowledge base.

Interview Question 11. Is there any other information you would like to provide regarding your experience with the management of risks before, during, or after the migration to the cloud? The final question asked by the interviewer asked each participant to provide any information concerning risk management and cloud migrations they thought to be relevant.

Each participant provided many different answers. The alignment of the participant's answers was with their function in the business. The participant answers described issues rather than risks. Further elaboration from the participants described events occurring after the completion of the migration. The participants asserted the following responses to the final question.

The overall value of risk mitigation is I think what they helped develop as part of the overall migration and the plan that everybody really felt comfortable with.

Testing after the risk mitigation is necessary with a greater emphasis after the migration is complete. In order to validate the mitigation was successful.

It is a security thing it's not having to constantly make sure that you've got the right servers and everything so you're able to offload some of those responsibilities to the provider of the services.

There is some economic impact in one hand. Your operating costs are going to go up.”

There's a lot of things that make the cloud attractive, but It's probably not 100 percent solution.

The technical risks are usually far far far fewer than the end user risks.

A lack of ability for people to effectively communicate with consultants that they bring in during these migrations to get them the tasks to complete the migration.

I think I took on a newfound appreciation for how important the risk management piece really was I think historically I may have viewed it as you know a layer of overhead that was required as part of the business and not truly appreciating its value.

Getting someone who is not involved in the cloud migration and getting them comfortable and onboard and understanding what the changes are and understanding why is far far far more important because they're either lack of involvement lack of understanding or the lack of communication and training will have them make more mistakes.

Summary

Chapter 4 of this research study presents a detailed review and analysis of the research data collected. Further, the identification and explanation of each source of data collection occurred. The participants were diverse from three businesses. Each participant worked in either a business management role or an IT function. All participants had direct experience with their firm's migration to the cloud.

All participant's interviews occurred using the Zoom conferencing software. The interviewer transcribed each participant's interview. The transcriptions were imported into the NVivo software to assist in defining the themes. Additionally, the interviewer analyzed each participant's responses using narrative analysis. The combination of the NVivo software and the narrative analysis by the interviewer provided correlative themes from the transcriptions. An analysis of this study's research question and the summarized results of the interview questions happened. Chapter 5 of this research study presents an evaluation of the research question, research purpose, contribution of the business technical problem, and recommendations for future research.

CHAPTER 5. CONCLUSIONS

Introduction

This chapter continues from Chapter 4 in a presentation of the results. A presentation of the analysis of the study results exists to check alignment with the research question for this study. Discussion of the evaluation of the research question and the fulfillment of the research purpose occurs. Further discussion covers the contribution to business technical problem and recommendations for further research. Finally, the presentation of the conclusions drawn from the entirety of the research was present.

Evaluation of Research Questions

This research study was to find answers to the research question: How do enterprise businesses in the United States manage the risks that they encounter during the migration of cloud computing? There was consistency in the answers provided by the participants. A prominent dichotomy between the business participants and the IT participants exists. The observation of variance in the participant answers occurs as a perceptual difference based on their respective operational involvement in the cloud migration activities. This evaluation of the research question condenses and presents the themes which emerged from the collected data.

Ho, Ocasio-Velázquez, and Booth (2017) asserted that the perception of users differs significantly, but there is a belief that the management of cloud computing will be performed. Each participant responding from the perspective of business management stated that other

operational teams, either internal or external, in the case of vendors, managed the risks. The business was relying on the operational group, either internal IT or external vendor, to perform all tasks relating to the management of the risks regarding cloud migration. The business management perspective of other groups managing risk was a reoccurring theme throughout the data.

The business participants provided advice and remained informed to the possibility of adverse issues but did not direct dialogues or inquiries into the risks of cloud migration. The business management participants relied on the information provided by external vendors to a greater extent than the internal IT groups. The approach the business participants responded was one of allowing the teams closest to the cloud migration to perform all tasks and work only from an advisory point of view.

Hsu and Lin (2015) asserted that IT groups' perception of risks differs from standard technology risks. The IT group had consistent expressions relating to the processes of risks in cloud migration. Each IT participant described direct involvement in risk management. The IT participants described a limited scope regarding risk management to include only technological issues and excluded business processes.

There is a greater reliance on external processes when managing cloud services, and this changes the approach of traditional IT groups (Hsu and Lin, 2015). All participants identified performing preemptive research before attempting the cloud migration. There were different and varying degrees of research introduced by the participants. The research described by the participants included the particular migration type, peer groups having already performed a similar migration and proof of concept at a limited scale. The preliminary research done by the

IT groups provided a scope in which the observation of risks would occur during the cloud migrations.

The risk management process the IT groups used consisted of a predetermined pattern. Initially, risks were identified and discussed as a topic in general meetings. Second, an assessment of each risk occurred. From the assessment, a determination of the ability of the risk to escalate and cause actual impairment to the cloud migration occurred. Finally, the adverse issues were mitigated rapidly without planning.

There was a reoccurring theme from the IT group when describing risks. The risks described were issues that had escalated when observed by the IT group. The IT group's perception of risk was an actual encounter with an escalated issue. The IT group was looking at actionable engagements and not the pre-assessment when describing cloud migration risks. The process of rapid mitigation was described by the IT group to be agile in its implementation of a solution. The speed of the migration was critical. IT participants indicated the importance of keeping the cloud migration tracking correctly to meet the implementation timeline.

Rahman et al. (2017) asserted that the need to have existing controls in place before cloud migration is fundamental. The outcome of the risk management process was, in every case, an informal list of the risks identified during the cloud migration. The participants described the capture of risks as both informal and limited to technical in scope. The IT participants elaborated relating a limited ability to compare a new risk to one that existed previously within the business.

A risk once raised to the level of an issue was noted in a taxonomy. A taxonomy tracking the mitigation and resolution of each risk rising to the level of an adverse issue occurred. The list of risks, issues, and mitigations were documented informally as an anecdotal set of

documentation. Upon further query, the retrieval of risk information occurred from email messages. Storing the risk information in email prevented a rapid method or process from searching for previous existing events. The participants described this as a regular occurrence when describing the documentation of risks. The discovery of the theme regarding risk documentation was apparent. Table 8 presents the principal risks identified by interviews, including the alignment to a business environment.

Table 8

List of Risks by Type

Risk	On-premise	Cloud
System Access		X
Security	X	X
Risk management		X
Cloud migration completion		X
Competing projects	X	X
Backup technologies		X
Rigid mitigation processes		X
Change of environment		X
Process changes		X
End-user ability to utilize cloud systems		X
Moving to the cloud to slowly	X	X
Cloud services fitting business needs		X
System performance in the cloud		X
Business planning versus IT planning	X	X
Business alignment with IT	X	X

The process of mitigation regarding the risks that became issues for the study population was limited. A single business encountered two of the three issues requiring management. One

business encountered no issues, and the final business encountered a single issue. Management of backup technology and business planning issues was swift. The IT group involved with backup and business planning issues acted directly to resolve each issue. Table 9 presents the three issues which escalated to the point of being managed.

Table 9

Risks that became Issues

Risk	On-Premise	Cloud	Mitigated
Backup Technology		X	X
Cloud Migration Business Planning	X	X	X
System Performance		X	X

In order to correct escalated issues efficiently, the correct controls must be in place before beginning cloud migration (Rahman et al., 2017). Corrective action taken by the IT group fixed the escalated backup issue. The issue discovered involved defects in the implementation.

The business planning issue was a complex issue that the senior IT manager managed with the corresponding business executives to create a cohesive alignment between the two units in the organization. The outcome was a new collaboration of the business unit and the IT technical group specific to cloud migration.

Management of the issue of system performance in the cloud occurred by the IT group and the external vendor providing services. Through the engagement of the SaaS provider, identification of defects in several controls occurred. The SaaS provider increased the performance through modification of the defective controls, creating a positive outcome.

The types of escalated issues described in the data are not uncommon. The possibility of issue escalation for the type of events witnessed is common enough to prepare for before cloud

migration. Extracting an existing risk framework from the internet to base a migration on is possible. The theme from the data on mitigation presents speed to migration over planning.

Fulfillment of Research Purpose

Chapter 5 presents information regarding the research study and the fulfillment of the research purpose. The purpose of this qualitative descriptive case study was to describe the processes of businesses in the United States use to manage risks during migration to cloud computing. An aggregation of the information captured from the participants of this research occurs. The participants represented multiple enterprise businesses within the United States. The businesses operate in different industries, but all businesses met this study's requirements for size and revenue. The results of this study can provide useful information for businesses in the future to identify possible risk strategies.

This research study followed a structured process. Chapter 1 defined the scope of the study. Chapter 2 presented a wide-ranging literature review conducted on the subject of the research study. A review of the academic and anecdotal literature provided the discovery of a gap in the knowledge concerning the area of experiential understanding of risk management related to cloud migrations. Chapter 3 outlined the design and methodology used to create a research study based on the gap in knowledge. Following the design and method of Chapter 3, including limiting the research to specific geographical areas and business categories, a case study aligned with the research question happened.

The research for this qualitative case study with multiple participants occurred. Each participant and business fulfilled the criteria scoped in Chapter 3. The participants included executive business management, IT management, both senior and mid-level, as well as IT practitioners. Each participant received the same questions. The questions were structured but

open-ended. Each participant was encouraged to provide as much information as they desired. The semi-structured interview with open-ended questions proved to be a valuable research method. The participants provided information within the scope of the interview question. Many participants went beyond the scope of the research question and elaborated, providing a more in-depth insight into their business processes.

Entry into the NVivo software occurred for all data collected through the research interviews for the assessment of common themes. Each participant transcript was read, evaluated, and analyzed, looking for common themes not presented by the NVivo software. It is worth noting that absent in each transcription was the identification of a formal risk management process.

The identification of themes from the interviews showed intent. A majority of the themes centered on risks, cloud migration, business processes, projects, and external vendors. These themes were repeated immediately between the first and second business. The third business contributions had direct alignment with the themes from businesses 1 and 2. The consistency of the responses from the gross population demonstrated data saturation. Further, the responses from the different perspectives of each business, including business management and IT management, confirmed the triangulation of the data from these different data points.

Contribution to Business Problem

This study surveys the business technical problem of limited knowledge of risk management during cloud migrations. United States businesses are attempting cloud migrations only to encounter risks that lead to the added cost. The cost increases of cloud migration stem from changes during the migration to avoid risks or mitigate risks that turned into adverse issues. The frameworks that exist for cloud migrations are plentiful (Fahmideh & Beydoun, 2017). The

utilization of complex frameworks that provide governance during cloud migration is not working.

There were many themes identified in the data in this study. The following is an outline of the main themes reflecting the management of risks:

- The business did not manage risks related to cloud migration.
- The IT group managed risks of the less complicated cloud migration.
- There existed an interchangeable concept of risks and issues.
- The use of external vendors occurred for management of the risks of complex cloud migration.
- Completion of the migration on time was a vital component.
- Capturing risk documentation was not a formal task.

The themes discovered in the data returned across the different businesses in their different industries. There was not a significant difference in the management of risks between the businesses. The three businesses managed risks and issues using similar methods.

This study occurred using information from three businesses. The businesses function in different industries, including healthcare, distribution, and retail. The similarities of the responses of risk management become visible across different businesses. The differences of the businesses provide a diversity of perspectives in the data results. Information from a broader perspective than a single industry provides relevance to the collected data. The data presented can be applied across multiple types of commerce without limitation to a single vertical.

Value exists for both academics and practitioners in the findings of this study in the domain of cloud migration. The purpose of this study was to fill the identified gap in knowledge

specific to the real world business management of risks during cloud migrations. This study fulfills its purpose through the descriptive presentation of multiple businesses' real world management of risks during cloud migration.

This study presented findings that the utilization of formal and sophisticated methodologies of risk management for cloud migration did not take place. The study presented the business's mitigation of adverse issues through rapid action with minimal planning. The findings exposed the need for the business to own and assess the risks and mitigation planning instead of outsourcing this practice. The findings further uncovered the necessity of capturing risks for future consideration of governance and controls in similar projects. These findings are valuable for businesses planning to perform cloud migration.

Recommendations for Further Research

This qualitative research case study was limited based on a specific geographical location and business category and attributes. Many businesses have a need and interest in performing a cloud migration that is outside of the demographics contained in this research study. These limitations alone provide for further research into businesses having performed migrations to cloud computing in different geographic areas and businesses of different sizes and scope. Additional research on risk management for businesses migrating from cloud computing back to an on-premise paradigm will provide valuable information from an opposite perspective.

Conclusion

Risk management in cloud computing migrations is a severe issue. Many businesses do not allocate and spend resources preparing for the risks of cloud migration. Businesses are reliant on external experts to perform risk management on cloud migrations rather than relying on internal resources. The creation of a formal yet light-weight risk framework that can be

applied by businesses would present a substantive change to cloud migrations. The ownership of cloud migration, along with risk management, could be carried out by internal IT groups.

Internal IT groups managing the cloud migration provides the opportunity for significant cost savings by removing external actors who do not have familiarity with the business.

REFERENCES

- Abbadi, I. M. (2013). A framework for establishing trust in cloud provenance. *International Journal of Information Security*, 12(2), 111-128. <https://doi.org/10.1007/s10207-012-0179-0>
- Adjei, J. K. (2015). Explaining the role of trust in cloud computing services. *Digital Policy, Regulation and Governance*, 17(1), 54-67. <https://doi.org/10.1108/info-09-2014-0042>
- Aleem, A., & Sprott, C. R. (2013). Let me in the cloud: Analysis of the benefit and risk assessment of cloud platform. *Journal of Financial Crime*, 20(1), 6-24. <https://doi.org/10.1108/13590791311287337>
- Alkhalil, A., Sahandi, R., & John, D. (2017). An exploration of the determinants for decision to migrate existing resources to cloud computing using an integrated TOE-DOI model. *Journal of Cloud Computing: Advances, Systems and Applications*, 6(2). <https://doi.org/10.1186/s13677-016-0072-x>
- Andriotis, A. (2018, February 9). Equifax hack might be worse than you think. *The Wall Street Journal*. Retrieved from <https://www.wsj.com/articles/equifax-hack-might-be-worse-than-you-think-1518191370>
- Attaran, M. (2017). Cloud computing technology: Leveraging the power of the internet to improve business performance. *Journal of International Technology and Information Management*, 26(1), 112-137. Retrieved from <https://iima.org/wp/jitim/>

- Bartoletti, D., Nelson, L. E., Herbert, L., Miller, P., Dai, C., Cser, A., & Kindness, A. (2017, November 7). *Predictions 2018: Cloud computing accelerates enterprise transformation everywhere. For Infrastructure & Operations Professionals*. Retrieved from <https://www.forrester.com>
- Battleon, D. A., West, B. C., Kim, J., Ramesh, B., & Robinson, P. S. (2016). Achieving dynamic capabilities with cloud computing: An empirical investigation. *European Journal of Information Systems*, 25(3), 209-230. <https://doi.org/10.1057/ejis.2015.12>
- Berger, J. O. (1985). *Statistical decision theory and Bayesian analysis* (2nd ed.). New York, NY: Springer Science+Business Media.
- Bromiley, P., McShane, M., Nair, A., & Rustambekov, E. (2015). Enterprise risk management: Review, critique, and research directions. *Long Range Planning*, 48(4), 265-276. <https://doi.org/10.1016/j.lrp.2014.07.005>
- Buchanan, R. (2008). Introduction: Design and organizational change. *Design Issues*, 24(1), 2-9. <https://doi.org/10.1162/desi.2008.24.1.2>
- Cámara, S. B., Fuentes, J. M., & Marín, J. M. (2015). Cloud computing, web 2.0, and operational performance the mediating role of supply chain integration. *The International Journal of Logistics Management*, 26(3), 426-458. <https://doi.org/10.1108/IJLM-07-2013-0085>
- Carcary, M., Doherty, E., & Conway, G. (2013). The adoption of cloud computing by Irish SMEs - an exploratory study. *Electronic Journal of Information Systems Evaluation*, 16(4), 258-269. Retrieved from <https://www.ejise.com/main.html>
- Carter, N., Bryant-Lukosius, D., DiCenso, A., Blythe, J., & Neville, A. J. (2014). The use of triangulation in qualitative research. *Oncology Nursing Forum*, 41(5), 545-547. <https://doi.org/10.1188/14.ONF.545-547>

- Cărutasu, N. L., & Cărutasu, G. (2016). Cloud ERP implementation. *FAIMA Business & Management Journal*, 4(1), 31-43. Retrieved from <https://www.faimajournal.ro/>
- Casassa-Mont, M., Matteucci, I., Petrocchi, M., & Sbodio, M. L. (2015). Towards safer information sharing in the cloud. *International Journal of Information Security*, 14(4), 319-334. <https://doi.org/10.1007/s10207-014-0258-5>
- Căţinean, I., & Căndea, D. (2013). Characteristics of the cloud computing model as a disruptive innovation. *Review of International Comparative Management*, 14(5), 783-803. Retrieved from <https://www.rmci.ase.ro/>
- Cho, V., & Chan, A. (2013, September 22). An integrative framework of comparing SaaS adoption for core and non-core business operations: An empirical study on Hong Kong industries. *Information Systems Frontiers*, 17, 629-644. <https://doi.org/10.1007/s10796-013-9450-9>
- Christensen, L., Johnson, R. B., & Turner, L. (2020). *Research methods, design, and analysis* (13th ed.) [VitalSource]. Retrieved from <https://www.pearson.com/>
- Cleary, P., & Quinn, M. (2016). Intellectual capital and business performance. *Journal of Intellectual Capital*, 17(2), 255-278. <https://doi.org/10.1108/JIC-06-2015-0058>
- Cloud migration market - Growth, trends, forecasts (2020 - 2025). (2020). Retrieved from https://www.researchandmarkets.com/research/dtzcmn/global_cloud?w=4
- Crampton, J. W. (2015, October 11). Collect it all: National security, big data and governance. *GEOJournal*, 80(4), 519-531. <https://doi.org/10.1007/s10708-014-9598-y>
- Creswell, J. W., & Creswell, J. D. (2018). *Research design: Qualitative, quantitative, and mixed methods approaches* (4th ed.). [VitalSource]. Retrieved from <https://us.sagepub.com>

- Creswell, J. W., & Poth, C. N. (2016). *Qualitative inquiry & research design: Choosing among five approaches* (4th ed.). [Kindle edition]. Retrieved from <https://us.sagepub.com>
- Cummings, S., Bridgman, T., & Brown, K. G. (2015). Unfreezing change as three steps: Rethinking Kurt Lewin's legacy for change management. *Human Relations*, 69(1), 33-60. <https://doi.org/10.1177/0018726715577707>
- Dantas, J., Matos, R., Araujo, J., & Maciel, P. (2015). Eucalyptus-based private clouds: Availability modeling and comparison to the cost of a public cloud. *Computing*, 97(11), 1121-1140. <https://doi.org/10.1007/s00607-015-0447-8>
- Debreceeny, R. S. (2013). Research on IT governance, risk, and value: Challenges and opportunities. *Journal of Information Systems*, 27(1), 129-135. <https://doi.org/10.2308/isis-10339>
- Debreceeny, R. S., & Gray, G. L. (2013). IT governance and process maturity: A multinational field study. *Journal of Information Systems*, 27(1), 157-188. <https://doi.org/10.2308/isis-50418>
- Dechouniotis, D., Dimolitsas, I., Papadakis-Vlachopapadopoulos, K., & Papavassiliou, S. (2018, June 25). Fuzzy multi-criteria based trust management in heterogeneous federated future internet testbeds. *future internet*, 10(58). <https://doi.org/10.3390/fi10070058>
- Dennehy, D., & Conboy, K. (2019, June 6). Breaking the flow: A study of contradictions in information systems development (ISD). *Information Technology & People*, 33(2), 477-501. <https://doi.org/10.1108/ITP-02-2018-0102>
- Department of Defense. (2013). DoD Information security program: Protection of classified information (NUMBER 5200.01, Vol 3). Retrieved from https://www.dodig.mil/Portals/48/Documents/Policy/520001_vol3.pdf

- Dionne, G. (2013). Risk management: History, definition, and critique. *Risk Management and Insurance Review*, 16(2), 147-166. <https://doi.org/10.1111/rmir.12016>
- Doherty, E., Carcary, M., & Conway, G. (2015). Migrating to the cloud: Examining the drivers and barriers to adoption of cloud computing by SMEs in Ireland: An exploratory study. *Journal of Small Business and Enterprise Development*, 22(3), 512-527. <https://doi.org/10.1108/JSBED-05-2013-0069>
- Domínguez-Mayo, F. J., García-García, J. A., Escalona, M. J., Mejías, M., Urbieto, M., & Rossi, G. (2015). A framework and tool to manage cloud computing service quality. *Software Quality Journal*, 23(1), 595-625. <https://doi.org/10.1007/s11219-014-9248-0>
- Eastburn, R. W., & Sharland, A. (2016, November 21). Risk management and managerial mindset. *The Journal of Risk Finance*, 18(1), 21-47. <https://doi.org/10.1108/JRF-09-2016-0114>
- Elezi, E., & Bamber, C. (2018). A guiding conceptual framework for individualized knowledge management model building. *Management Dynamics in the Knowledge Economy*, 6(3), 343-369. <https://doi.org/10.25019/MDKE/6.3.01>
- Fahmideh, M., & Beydoun, G. (2017, December 15). Reusing empirical knowledge during cloud computing adoption. *The Journal of Systems and Software*, 138, 124-157. <https://doi.org/10.1016/j.jss.2017.12.011>
- Farah, B. N. (2015). Strategies for deploying business applications on the cloud. *Journal of Management Policy and Practice*, 16(4), 30-42. Retrieved from <https://www.na-businesspress.com/jmppopen.html>

- Gahin, M. F. (1967). A theory of pure risk management in the business firm. *Journal of Risk & Insurance*, 34(1), 121-130. <https://doi.org/10.2307/251020>
- Gartner. (2016). *2017 Planning guide for cloud computing*. Retrieved from <https://www.gartner.com/en/documents/3471551/2017-planning-guide-for-cloud-computing>
- Gartner. (2017). *Cloud strategy leadership*. Retrieved from https://www.gartner.com/imagesrv/books/cloud/cloud_strategy_leadership.pdf
- Gartner. (2018). *IT glossary*. Retrieved from <https://www.gartner.com/>
- Goel, R. (2015). Trusted supply chains: Surveying competitive value of the cloud. *International Journal of Management & Information Systems*, 19(1), 43-50. <https://doi.org/10.19030/ijmis.v19i1.9087>
- Graziotin, D., Fagerholm, F., Wang, X., & Abrahamsson, P. (2018, February 20). What happens when software developers are (un)happy. *The Journal of Systems and Software*, 140, 32-47. <https://doi.org/10.1016/j.jss.2018.02.041>
- Gutierrez, A., Boukrami, E., & Lumsden, R. (2015). Technological, organisational and environmental factors influencing managers' decision to adopt cloud computing in the UK. *Journal of Enterprise Information Management*, 28(6), 788-807. <https://doi.org/10.1108/JEIM-01-2015-0001>
- Hill, C. W. (2016). *Strategic management: Theory: An integrated approach* (12th ed.) [VitalSource]. Retrieved from <https://www.cengage.com>
- Ho, S. M., Ocasio-Velázquez, M., & Booth, C. (2017, August 12). Trust or consequences? Causal effects of perceived risk and subjective norms on cloud technology adoption. *Computers & Security*, 70, 581-595. <https://doi.org/10.1016/j.cose.2017.08.004>

- Hsu, C., & Lin, J. C. (2015, December 21). Factors affecting the adoption of cloud services in enterprises. *Information Systems and e-Business Management*, 14, 791–822.
<https://doi.org/10.1007/s10257-015-0300-9>
- ISACA. (2014). Controls and assurance in the cloud: Using COBIT 5. Retrieved from <https://www.isaca.org/>
- Islam, S., Fenz, S., Weippl, E., & Mouratidis, H. (2017, February 22). A risk management framework for cloud migration decision support. *Journal of Risk and Financial Management*, 10(10). <https://doi.org/10.3390/jrfm10020010>
- Jaeger, C. (2016, June 27). The coming breakthrough in risk research. *Economics*, 10(16), 1-29.
<https://doi.org/10.5018/economics-ejournal.ja.2016-16>
- Jede, A., & Teuteberg, F. (2016). Investigating preconditions for a financially advantageous cloud usage. *International Journal of Accounting and Information Management*, 24(2), 116-134. <https://doi.org/10.1108/IJAIM-04-2015-0018>
- Jennings, B., & Stadler, R. (2015). Resource management in clouds: Survey and research challenges. *Journal of Network and Systems Management*, 23, 567-619.
<https://doi.org/10.1007/s10922-014-9307-7>
- Kajiyama, T., Jennex, M., & Addo, T. (2017, September 8). To cloud or not to cloud: How risks and threats are affecting cloud adoption decisions. *Information & Computer Security*, 25(5), 634-659. <https://doi.org/10.1108/ICS-07-2016-0051>
- Khalil, S. (2019). Adopting the cloud: how it affects firm strategy. *The Journal of Business Strategy*, 40(4), 28-35. <https://doi.org/10.1108/JBS-05-2018-0089>
- Karunakaran, S., Krishnaswamy, V., & Rangaraja, S. P. (2015). Business view of cloud: Decisions, models and opportunities - a classification and review of research.

- Management Research Review*, 38(6), 582-604. <https://doi.org/10.1108/MRR-01-2014-0021>
- Kauffman, R. J., Ma, D., & Yu, M. (2016, February 6). A metrics suite of cloud computing adoption readiness. *Electron Markets*, 28, 11-37. <https://doi.org/10.1007/s12525-015-0213-y>
- Kosalge, P. U. (2015). Finding the tipping point for a CEO to say yes to an ERP: A case study. *Journal of Enterprise Information Management*, 28(5), 718-738. <https://doi.org/10.1108/JEIM-07-2014-0073>
- Kratzke, N., & Quint, P. C. (2017, January 5). Understanding cloud-native applications after 10 years of cloud computing - A systematic mapping study. *Journal of Systems and Software*, 126, 1-16. <https://doi.org/10.1016/j.jss.2017.01.001>
- Kushida, K. E., Murray, J., & Zysman, J. (2015). Cloud computing: From scarcity to abundance. *Journal of Industrial Computer Trade*, 15, 5-19. <https://doi.org/10.1007/s10842-014-0188-y>
- Leedy, P. D., & Ormrod, J. E. (2018). *Practical research: Planning and design* (12 ed.) [VitalSource]. Retrieved from <https://www.pearson.com/>
- Lewin, K. (1947). Field theory in social science: Selected theoretical papers by Kurt Lewin. *International Journal of Group Psychotherapy*, 1(4), 388-389. <https://doi.org/10.1080/00207284.1951.11507900>
- Link, B., & Back, A. (2015, March 11). Classifying systemic differences between software as a service- and on-premise-enterprise resource planning. *Journal of Enterprise Information Management*, 28(6), 808-837. <https://doi.org/10.1108/JEIM-07-2014-0069>

- Lundqvist, S. A. (2015). Why firms implement risk governance - Stepping beyond traditional risk management to enterprise risk management. *Journal of Accounting and Public Policy*, 34(5), 441-466. <https://doi.org/10.1016/j.jaccpubpol.2015.05.002>
- Lynn, T., Van Der Werff, L., Hunt, G., & Healy, P. (2016). Development of a cloud trust label: A delphi approach. *The Journal of Computer Information Systems*, 56(3), 185-193. <https://doi.org/10.1080/08874417.2016.1153887>
- Mackita, M., Shin, S., & Choe, T. (2019). ERMOCTAVE: A risk management framework for IT systems which adopt cloud computing. *Future Internet*, 11(9). <https://doi.org/10.3390/fil1090195>
- Mahy, Y., Ouzzif, M., & Bouragba, K. (2016). Toward a shared view of IT governance. *International Journal of Innovation, Management and Technology*, 7(4), 125-131. <https://doi.org/10.18178/ijimt.2016.7.4.658>
- Maramwidze-Merrison, E. (2016). Innovative methodologies in qualitative research: Social media window for accessing organisational elites for interviews. *Electronic Journal of Business Research Methods*, 14(2), 157-167. Retrieved from <https://www.ejbrm.com>
- Markolf, S. A., Klima, K., & Wong, T. L. (2015, October 19). Adaptation frameworks used by US decision-makers: A literature review. *Environment Systems and Decisions*, 35(4), 427-436. <https://doi.org/10.1007/s10669-015-9572-3>
- Meier, K. J., Favero, N., & Zhu, L. (2015, January 7). Performance gaps and managerial decisions: A Bayesian decision theory of managerial action. *Journal of Public Administration Research and Theory*, 25(4), 1221-1246. <https://doi.org/10.1093/jopart/muu054>

- Merriam, S. B., & Tisdell, E. J. (2016). *Qualitative research a guide to design and implementation* (4 ed.) [Kindle]. Retrieved from www.wiley.com
- Mickahail, B. (2015). Corporate implementation of design thinking for innovation and economic growth. *Journal of Strategic Innovation and Sustainability*, 10(2), 67-79. Retrieved from <https://www.na-businesspress.com/jsisopen.html>
- National Institute of Standards and Technology. (2004). Standards for security categorization of federal information and information systems (NIST FIPS Special Publication 199). <https://doi.org/10.6028/NIST.FIPS.199>
- National Institute of Standards and Technology. (2011). Final version of NIST cloud computing definition published. Retrieved from <https://www.nist.gov/>
- National Institute of Standards and Technology. (2013). *NIST cloud computing standards roadmap* (NIST Special Publication 500-291, Version 2). Washington, DC: Government Printing Office.
- Nicho, M., & Khan, S. (2017). IT governance measurement tools and its application in IT business alignment. *Journal of International Technology and Information Management*, 26(1), 81-111. Retrieved from <https://scholarworks.lib.csusb.edu/jitim/>
- Nicho, M., & Muamaar, S. (2016). Towards a taxonomy of challenges in an integrated IT governance framework implementation. *Journal of International Technology and Information Management*, 25(2), 1-31. Retrieved from <https://iima.org/wp/jitim/>
- Patrignani, N., & Kavathatzopoulos, I. (2015). Cloud computing: The ultimate step towards the virtual enterprise? *Special Interest Group Computers and Society*, 45(3), 68-72. Retrieved from <https://www.sigcas.org/>

- Pick, R. A. (2015). Shepherd or servant: Centralization and decentralization in information technology governance. *International Journal of Management & Information Systems (Online)*, 19(2), 61-68. <https://doi.org/10.19030/ijmis.v19i2.9173>
- Priyadarshinee, P., Raut, R. D., Jha, M. K., & Gardas, B. B. (2017, July 26). Understanding and predicting the determinants of cloud computing adoption: A two staged hybrid SEM - neural networks approach. *Computers in Human Behavior*, 76, 341-362. <https://doi.org/10.1016/j.chb.2017.07.027>
- Rahman, A. A., Islam, S., Kalloniatis, C., & Gritzalis, S. (2017). A risk management approach for a sustainable cloud migration. *Journal Risk Financial Management*, 10(4), 1-20. <https://doi.org/10.3390/jrfm10040020>
- Ray, D. (2016). Cloud adoption decisions: Benefitting from an integrated perspective. *Electronic Journal Information Systems Evaluation*, 19(1), 3-21. Retrieved from <https://www.ejise.com/>
- Saldaña, J. (2015). *The coding manual for qualitative researchers* (3 ed.). [VitalSource]. Retrieved from <https://us.sagepub.com>
- Sankararajan, D., & Shrivastava, N. K. (2012). Risks vs. issues. *PM Network*, 26(6), 28-29. Retrieved from <https://www.pmi.org>
- Sarayreh, B. H., Khudair, H., & Barakat, E. A. (2013). Comparative study: The Kurt Lewin of change management. *International Journal of Computer and Information Technology*, 2(4), 626-629. Retrieved from <https://www.ijcit.com/>
- Schindler, P. S. (2019). *Business research methods* (13th ed.). [VitalSource]. Retrieved from <https://www.mhhe.com>

- Schlosser, F., Beimborn, D., Weitzel, T., & Wagner, H. (2015). Achieving social alignment between business and IT - an empirical evaluation of the efficacy of IT governance mechanisms. *Journal of Information Technology, suppl. Special Issue: Revisiting Strategic Alignment 25 Years On*, 30(2), 119-135. <https://doi.org/10.1057/jit.2015.2>
- Schneider, S., & Sunyaev, A. (2015). CloudLive: A life cycle framework for cloud services. *Electron Markets*, 25(1), 299-311. <https://doi.org/10.1007/s12525-015-0205-y>
- Schneider, S., & Sunyaev, A. (2016). Determinant factors of cloud-sourcing decisions: Reflecting on the IT outsourcing literature in the era of cloud computing. *Journal of Information Technology*, 31(1), 1-31. <https://doi.org/10.1057/jit.2014.25>
- Seethamraju, R. (2014, May 27). Adoption of software as a service (SaaS) enterprise resource planning (ERP) systems in small and medium sized enterprises (SMEs). *Information Systems Frontiers*, 17(3), 475-492. <https://doi.org/10.1007/s10796-014-9506-5>
- Simon, H. A. (1955). A behavioral model of rational choice. *The Quarterly Journal of Economics*, 69(1), 99-118. <https://doi.org/10.2307/1884852>
- Simon, H. A. (1996). *The sciences of the artificial* (3rd ed.). [Kindle edition]. Retrieved from <https://mitpress.mit.edu/>
- Simon, H. A. (1997). *Administrative behavior: A study of decision-making processes in administrative organizations* (4th ed.). [Kindle edition]. Retrieved from <https://www.simonandschuster.com/>
- Slovic, P. (2016). *The perception of risk*. [VitalSource]. Retrieved from www.taylorfrancis.com
- Stake, R. E. (2010). *Qualitative research: Studying how things work*. [Kindle]. Retrieved from www.guilford.com

Thomas, M. (2017). Use multiple guidance systems for effective governance. Retrieved from <https://www.isaca.org/>

U.S. Department of Health and Human Services, National Commission for the Protection of Human Subjects of Biomedical and Behavioral Research. (1979). *The Belmont report: Ethical principles and guidelines for the protection of human subjects of research* (45 CFR 46). Retrieved from <http://www.hhs.gov/ohrp/regulations-and-policy/belmont-report/>

U.S. Department of Labor, Bureau of Labor Statistics. (2018). *Occupational Outlook Handbook*. Retrieved from <https://www.bls.gov/bls/infohome.htm>

van Wyk, J., & Rudman, R. (2019). COBIT 5 compliance: Best practices cognitive computing risk assessment and control checklist. *Meditari Accountancy Research*, 27(5), 761-788. <https://doi.org/10.1108/MEDAR-04-2018-0325>

Vidal, G. G., Rodríguez, A. S., Campdesuñer, R. P., & Vivar, R. M. (2017). Strategic choices of an entrepreneur using statistical decision theory. *Journal of International Business and Economics*, 5(1), 75-84. <https://doi.org/10.15640/jibe.v5n1a7>

Vision Solutions. (2017). *2017 State of the resilience report* [Industry Survey]. Retrieved from <https://www.visionsolutions.com/2017SOR>

Von Solms, R., & Willett, M. (2017). Cloud computing assurance - A review of literature guidance. *Information and Computer Security*, 25(1), 26-46. <https://doi.org/10.1108/ICS-09-2015-0037>

Westerman, G., & Hunter, R. (2007). *IT risk turning business threats into competitive advantage*. Boston, MA: Harvard Business School Press.

- Wilkin, C. L., Campbell, J., & Moore, S. (2013). Creating value through governing IT deployment in a public/private-sector inter-organisational context: A human agency perspective. *European Journal of Information Systems*, 22(5), 498-511.
<https://doi.org/10.1057/ejis.2012.21>
- Yin, R. K. (2014). *Case study research design and methods* (5 ed.). [Kindle]. Retrieved from <https://us.sagepub.com>
- Zota, D. R., & Fratila, A. L. (2013). Cloud standardization: Consistent business processes and information. *Informatica Economica*, 17(3), 137-147.
<https://doi.org/10.12948/issn14531305/17.3.2013.12>

Appendix

Research Interview Questions

Interview Questions

Interview Question 1. Can you provide the date of the migration?

Interview Question 2. Was there a name for this migration or project?

Interview Question 3. (Pre-cloud migration) Were there meetings to manage the risks?

Interview Question 4. (Pre-cloud migration) What was your role in risk management at your organization before cloud migration?

Interview Question 5. What did your firm do to identify risks associated with the cloud migration specifically, and did your firm use the same process before the migration to manage risks of the cloud migration? If the process was different, what changed?

Interview Question 6. What role did you play in the management of risks during the migration to cloud computing?

Interview Question 7. Were there meetings to manage the risks of cloud migration, and if so, who attended the risk management meetings?

Interview Question 8. What role did you play in the management of risks during the migration to cloud computing, and did you identify risks during the migration to cloud computing?

Interview Question 9. Who was responsible for the management of adverse events for your firm during the migration to cloud computing?

Interview Question 10. Was a knowledge base or other area of notes taken on the management of adverse events during the migration to cloud computing?

Interview Question 11. Is there any other information you would like to provide regarding your experience with the management of risks before, during, or after the migration to the cloud?