2019

Adoption of Cloud Computing Services in an Illinois-Based Insurance Company

Nekerral Polk
Walden University

Walden University

College of Management and Technology

This is to certify that the doctoral study by

Nekerral Polk

has been found to be complete and satisfactory in all respects,
and that any and all revisions required by
the review committee have been made.

Review Committee
Dr. Charlie Shao, Committee Chairperson, Information Technology Faculty
Dr. Steven Case, Committee Member, Information Technology Faculty
Dr. Gary Griffith, University Reviewer, Information Technology Faculty

Chief Academic Officer
Eric Riedel, Ph.D.

Walden University
2019

Abstract

Adoption of Cloud Computing Services in an Illinois-Based Insurance Company

by

Nekerral Polk

MS, University of Dallas, 2008

BBA, Middle Tennessee State University, 1994

Doctoral Study Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Information Technology

Walden University

May 2019

Abstract

The decision to adopt cloud computing services should involve business units of an insurance company as well as information technology (IT) because cloud computing services are viewed as both a technology offering and business alternative. The purpose of this qualitative exploratory case study was to explore the strategies used by IT architects of an Illinois-based insurance company when adopting cloud computing services. The theory supporting this study was the technology acceptance model. The study's population consisted of IT architects from an Illinois-based insurance company that have used strategies to adopt cloud computing services. This study's data collection included semistructured interviews and review of organizational documents. Member checking with each participant increased the validity of this study's findings. Four major themes emerged from this study: strategies to adopt cloud computing services, strategies to adopt cloud services models, strategies to adopt cloud computing models, and concerns affecting the strategies to adopt cloud computing services. The study findings may assist IT architects in developing effective strategies to adopt cloud computing services for their respective business unit. This study might serve as a foundation for positive social change by decreasing customer concerns regarding critical information being compromised when adopting cloud computing services.

Adoption of Cloud Computing Services in an Illinois-Based Insurance Company

by

Nekerral Polk

MS, University of Dallas, 2008

BBA, Middle Tennessee State University, 1994

Doctoral Study Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Information Technology

Walden University

May 2019

Dedication

I am dedicating this study to the special education community and people with learning disabilities. There are many times when people with learning disabilities are overlooked or told they cannot do something. I want everyone in the special education community to continue moving forward and never backwards. There will be times when we need to sidestep to get around obstacles, but we must strive to do our best and keep moving forward.

Acknowledgments

I want to thank Dr. Brenda Washington, Dr. Sharonda Johnson, and Dr. Shane Williams for being there to help lift my spirits when I became discouraged and wanted to stop. I want to thank my mother most of all because she believed in me when my teachers told me college was not for me. It was her belief in me that made me attend college and continue to seek knowledge and understanding. I want to extend a special thank you to my committee, committee chair Dr. Charlie Shao, my second committee member, Dr. Steven Case, and university research reviewer (URR), Dr. Gary Griffin.

Table of Contents

List of Tables

Section 1: Foundation of the Study

The decision to adopt cloud computing services should involve business units of an insurance company as well as information technology (IT) because cloud computing services are viewed as both a technology offering and business alternative (Iyer, Krishnan, Sareen, & Panda, 2013). Cloud computing services emerged as an area of interest in business because of ideas such as pay as you go services. With a simplified pay as you go usage policy, the adoption of cloud computing services offers adopters capabilities such as barebones infrastructure, test environments, and full software packages with minimal investments by consumers (Jede & Teuteberg, 2016; Ruoning & Palvia, 2013). The adoption of cloud computing services has allowed IT architects to reduce their upfront costs and blur the traditional lines between technology and the business. Additionally, IT architects have the ability to deploy computational tools rapidly and respond more quickly to changing market needs (Oliveira, Thomas, & Espadanal, 2014; Tarmidi, Rasid, Alrazi, & Roni, 2014). Some IT architects view cloud computing services as a technology offering and business solution alternative to on-premise solutions, but their reasons for adopting cloud computing services are driven more by economic rationale than by technology justifications. Additionally, IT architects view cloud computing services as a merger of state of the art concepts like virtualization, server consolidation, interoperability, and dynamic central processing unit (CPU) provisioning (Iyer et al., 2013). Thus, the decision of an IT architect to adopt cloud computing services is more than a technology offering and business alternative to on-premise solutions.

In this section of the study, I include the background of the problem, problem statement, purpose statement, nature of the study, research question, and conceptual framework of the study. Definitions of terms, assumptions, limitations, delimitations, and significance of the study are also included in this section. In the review of academic and professional literature section, I include research and professional work focused on the adoption of cloud computing services.

Background of the Problem

Technology efficiency, business agility, scalable hardware, and software resources are key factors IT architects consider when adopting cloud computing services. The adoption of cloud computing services has the capacity to seamlessly deliver IT functions with a proven viable and cost-effective model (Oliveira et al., 2014). The benefit of using rapid elasticity and scalability for enterprise applications allows users to log on anytime from anywhere with an internet connection (Wang, Wood, Abdul-Rahman, & Lee, 2016). An IT architect's decision to adopt cloud computing services is usually driven by a business decision to lower operating expenses, but there are other concerns involved such as security, complexity, regulatory compliance, and a cloud implementation strategy. An effective risk-based approach will allow everyone involved in a decision to adopt cloud computing services to differentiate between operational and regulatory compliance risks (Novkovic & Korkut, 2017). Furthermore, using an effective risk-based approach will allow IT architects to consider all options before making a decision to adopt cloud computing services.

If an IT architect wishes to adopt cloud computing services, an overall strategy is required along with a strategy for each application moving to the cloud. Defining a clear strategy for adopting cloud computing services allows IT architects to think about business costs if an application is not available or suffers a data breach (Doherty, Carcary, & Conway, 2015). During the literature review, articles were found to define an IT strategy to address security and regulatory compliance allowing IT architects to meet business goals in an Illinois-based insurance company.

Problem Statement

Akar and Mardiyan (2016) indicated that cloud computing services became one of the most versatile technology services offered with 60% of an organization's IT infrastructure being hosted by a cloud service provider. However, the overall adoption of cloud computing remains low because 36% of IT architects have a no strategy plan and fail to adopt cloud computing services (Aharony, 2015; Goutas, Sutanto, & Aldarbesti, 2016). The general IT problem is that some companies fail in the adoption of cloud computing services. The specific IT problem is that some IT architects lack strategies to adopt cloud computing services.

Purpose Statement

The purpose of this qualitative exploratory case study was to explore the strategies used by IT architects of an Illinois-based insurance company when adopting cloud computing services. The target population of this exploratory case study were IT architects of an Illinois-based insurance company. Each participant had a minimum of 5 years of experience in their respective field and possessed the authority to impact

decisions concerning cloud computing services adoption. The results of this study may provide other IT architects with valuable insights into specific strategies to improve their cloud computing services implementation. This study will contribute to social change by supporting the development of sustainable business models used to reduce infrastructure costs, increase flexibility, and improve business capability. Additionally, an implication of this study for positive social change is that IT architects in an insurance company can help reduce carbon emissions by using a multitenant cloud solution versus a brick and mortar data center.

Nature of the Study

During this study, a qualitative methodology was used to gain an understanding of underlying reasons, motivations, and opinions contributing to a social or human problem. A qualitative methodology was appropriate for this study because the intent of the study was to investigate the professional thoughts and opinions of the research participants. A quantitative methodology is primarily used to quantify a problem by generating numerical data that is transformed into useable statistics for hypothesis testing (Scrutton & Beames, 2015). A quantitative methodology was not appropriate for this research since hypothesis testing was not involved. A mixed methodology is a combination of both qualitative and quantitative methods and allows the investigation of a research problem using two different methods. A survey using close-ended questions to collect data for a phenomenon did not occur in my research; therefore, a mixed methodology was not warranted.

The design chosen for this study was the exploratory case study design because it is used to analyze a person, events, decisions, or policies. A case study requires multiple sources of information such as interviews, participant observations, documents, and questionnaires (Yin, 2014). A phenomenological design uses lived experiences and perceptions to determine new knowledge from participants (Moustakas, 1994). The research performed in this study did not focus on the essence of a lived experience; therefore, a phenomenological design was not used. Ethnography design involves research to analyze social interactions by examining shared patterns of behaviors, beliefs, and language in a cultural group (Thornham & Cruz, 2018). The research performed in this study did not examine shared patterns of behavior, beliefs, and language in a cultural group; thus, an ethnography design was not used. The narrative design involves data collection from multiple sources to provide deep and profound insights into social representations of participants (Palvia, Baqir, & Nemati, 2018). The research performed in this study did not collect data from multiple sources to provide a deeper or more profound insights; consequently, a narrative design was not used. An exploratory case study design was used to obtain data for this study through interviews, document analysis, and participant observations.

Research Question

What strategies do IT architects of an Illinois-based insurance company use to adopt cloud computing services?

Interview Questions

Semistructured interview questions were used to collect data from participants. The goal of each question was to extract vital information to help answer the research question. By using semistructured main questions followed by a probing question, this study gathered additional information from each participant. The interview questions were as follows:

Demographic Questions

1. What is your role in the organization?
2. How long have you been in your current role?
3. How many years of experience do you have as an IT architect?
4. Do you have the authority to impact decisions concerning strategies for adopting cloud computing services for your respective business unit?

Interview Questions

1. What strategies have you used to adopt cloud computing services? How would you describe the usefulness of those strategies in terms of the overall success of adopting cloud computing services?
2. What strategies did you use that were least effective in the adoption of cloud computing services? What made the strategies least effective? How easy were those strategies to implement?
3. What strategies did you use that were most effective in the adoption of cloud computing services? What made the strategies most effective? How easy were those strategies to implement?

4. What other strategies did you use that were effective in the adoption of cloud computing services? What made the other strategies effective? How easy were those strategies to implement?
5. In your experience, what issues prohibited cloud computing services adoption from being successful? Why did the issues prohibit the adoption from being successful?
6. What was your main concern in your strategy to adopt cloud computing services? Why did you have the concern? How easy was the concern to resolve? What additional information is beneficial to add concerning IT strategies used to adopt cloud computing services?

Conceptual Framework

The technology acceptance model (TAM) was used during this study. In 1986, Fred Davis developed the TAM based on an adaptation of the theory of reasoned action (TRA) to the field of Information Systems. The theory of reasoned action explains the relationship between attitudes and behaviors within human action. The TAM focuses on perceived usefulness (PU) and perceived ease of use (PEOU) defined by an individual's intention to use a system. Perceived usefulness is defined as being the degree to which a person believes that the use of a system will improve his performance. Perceived ease of use refers to the degree to which a person believes that the use of a system will be effortless. PU is also viewed as a byproduct of PEOU. To avoid the attitude construct found in the TRA, researchers such as Fred Davis and Richard Bagozzi simplified the TAM by removing such constructs. Both the TRA and TAM have strong behavioral

elements indicating an individual's intention to act and have the appropriate autonomy without limitations. Limitations such as limited ability, time, environmental, or organizational may impact using TAM to determine a user intent to adopt a new technology (Davis, Bagozzi, & Warshaw, 1989). Although the TAM has certain limitations, it was appropriate for this study.

The TAM was appropriate for this study because the TAM focuses on PU and PEOU as the main determinants of an individual's intention to adopt new technology. For example, moving from a local data center to a cloud service provider (CSP) with ease could be considered as PEOU. If migrating applications to the cloud is cumbersome, an IT architect may decide to stay on premise and not take advantage of the benefits provided by cloud computing service adoption. Having the ability to use pay as you go pricing and expanding during peak processing times could be considered PU.

Definition of Terms

The definitions used in this study are industry specific terms which may not be clear or known by the reader. Each definition will add clarity and context for the reader as well as provide additional objectivity to the goals of this study.

Anything as a Service (XaaS): Anything as a service is a concept provided by a cloud service provider allowing customers to replace the "X" with any letter indicating another service. If databases and communications were hosted in the cloud they could be referenced as Database as a Service (DBaaS) and Unified Communication as a Service (UCaaS). The latest trend is Cache as a Service (CaaS) which is a method used by search

engines to minimize input/output of their search algorithms and thus improve performance (Ribas et al., 2015).

Cloud Computing Services: Cloud computing services are resources that are ubiquitous, convenient, and provide on demand network access to a shared pool of configurable computing resources (Mac-Anigboro & Usoro, 2015).

Community Cloud: A community cloud is classified as distributed infrastructure for a specific group or business partner to share resources (Maqueira-Marín, Bruque-Cámara, & Minguela-Rata, 2017).

Hybrid Cloud: A hybrid cloud system is defined as two or more distinct cloud systems in one homogeneous system (Wu & Feng-Kwei, 2015). A hybrid cloud system may incorporate public, private, and community clouds. A hybrid cloud solution allows critical applications or systems containing sensitive data running on infrastructure in a private data center to be extended to an external cloud (Shakir, Abubakar, Yousoff, Waseem, & Al-Emran, 2016).

Infrastructure as a Service (IaaS): Infrastructure as a service is the cloud computing model used with infrastructure such as storage, servers, and central processing through the use of virtual machines (Shin, Jo, Lee, & Lee, 2014). IaaS is one of the fastest growing fields because a cloud service provider can combine virtual machines and data storage into one platform with minimal resource management (Arsovski, Arsovski, Stefanović, Tadić, & Aleksić, 2017).

Multitenancy: A multitenancy cloud solution is a cloud service offering where simultaneous users are collocated in the same cloud architecture (Surendro, Supriana, & Supriana, 2016).

Platform as a Service (PaaS): Platform as a service is the cloud computing model that provides a customer with a highly integrated environment consisting of an operating system, hardware, and network (Daylami, 2015).

Private Cloud: A private cloud contains data and processes managed by an IT department in an organization. A private cloud is not limited by network, security, or legal restrictions that may impact a public cloud (Davidovic, Ilijevic, Luk, & Pogarcic, 2015).

Public Cloud: A public cloud is defined as a cloud offering maintained for generic public use by a third-party entity. The third-party entity may be an academic organization, business, statecraft organization, or a mixture of all three (Kaul, Sood, & Jain, 2017).

Software as a Service (SaaS): Software as a service is the cloud computing model where the customer uses a service provider's application running on cloud infrastructure (Koo & Kim, 2015). The underlying cloud infrastructure is not managed by the application provider or the customer but by the cloud service provider (Kung, Cegielski, & Kung, 2015).

Assumptions, Limitations, and Delimitations

Primary and secondary data sources were used in this study. Resources included interviews with IT architects, scholarly journals, and peer reviewed articles from Walden

University's library. The sources contributed assumptions as well as limitations and delimitations in the study.

Assumptions

Assumptions are important to understand in qualitative research. Assumptions are facts that anyone reading this study will assume are true based on population, research design, and statistical tests (Yin, 2014). An assumption was made that each participant understood the impact of cloud computing services, cloud security, loss of data, regulatory compliance concerns, and personal privacy. Another assumption of this study was that participants' attitudes, experiences, and behaviors were reflected honestly when they answered the interview questions. An additional assumption pertains to strategies in this study representing the experiences of IT architects within their respective business unit.

Limitations

Limitations are potential weaknesses in a study that are typically out of the researcher's control. Limitations may include but are not limited to the choice of research design and statistical model. Additionally, limitations are restrictions on a study that are not easily dismissed (Kirkwood & Price, 2013). Research for this study was limited to an Illinois-based insurance company with a participation population focused within the Illinois area. Additionally, limiting the study to Illinois limited the sample size of the study. Without an adequate sample size, the research may be considered incomplete or invalid. Another limitation was that participants may have answered questions based on

corporate policy versus factual information. Some participants may have feared repercussion from the company and opted out of participating in the study.

Delimitations

Delimitation are considered the set boundaries for a research study. A researcher may also use delimitations to narrow the scope of their study to help guarantee completion of research (Svensson & Doumas, 2013). First, all participants of this study had an IT architect role with an understanding of cloud computing services. Additionally, each participant had authority to impact decisions concerning strategies for adopting cloud computing services for their respective business unit. Therefore, IT architects who did not have authority to impact decisions concerning the adoption of cloud computing services were excluded.

The population of this study was limited to a specific company in Illinois. Furthermore, the scope limits the sample to a confined area which may lead to future studies. Finally, there was not a differentiation between large, midsized, or small business units adopting cloud computing services.

Significance of the Study

Contribution to IT Practice

Research for this study could potentially address gaps in IT practices regarding the adoption of cloud computing services for an Illinois-based insurance company. Factors such as the Health Insurance Portability and Accountability Act (HIPAA), Personal Identifiable Information (PII), Personal Card Industry Data Security Standards (PCI-DSS), and Sarbanes-Oxley Act (SOX) may influence an IT architect’s decision to

adopt cloud computing services. HIPAA was created to modernize the flow of healthcare information, stipulate how PII maintained by the healthcare and healthcare insurance industries should be protected from fraud, theft, and address limitations on healthcare insurance coverage (Phaphoom, Wang, Samuel, Helmer, & Abrahamsson, 2015). PII is defined as any information about an individual maintained by an agency, including any information that can be used to distinguish or trace and individual's identity (A. Ghorbel, M. Ghorbel, & Jmaiel, 2017). PCI-DSS is an information security standard for organizations that handle branded credit cards from the major card schemes (Grozev & Buyya, 2016). Sox is a United States federal law that set new or expanded requirements for all U.S. public company boards, management, and public accounting firms (Tang & Liu, 2015).

IT architects must have an understanding of data security and where a specific cloud service provider's infrastructure is located. Compliance laws prevent certain data from being stored outside of the continental United States (Juels & Oprea, 2013). Therefore, an insurance company may establish strategies to address regulatory compliance concerns impacting the adoption of cloud computing services.

Implications for Social Change

This qualitative exploratory case study may impact social change because insurance companies and consumers are leery of cloud computing services due to security concerns. The research can provide strategies for other insurance companies adopting cloud computing services to benefit from IT efficiencies and business agility. For example, an insurance company can use cloud computing services to maximize IT

resources without the overhead of a traditional data center. By maximizing IT resources via a cloud service provider, an insurance company can move to a pay as you go system and pass on the savings to the customer.

Additionally, adopting cloud computing services allows IT architects in an insurance company to become environmentally friendly. Carbon emissions may be reduced if IT architects in insurance companies use a multitenant cloud solution versus a brick and mortar data center. For example, Google's data center consumes 1120 GWh equating to $67 million dollars annually and Microsoft consumes 600 GWH equating to $36 million dollars annually. In fact, generating 100 MWh in the U.S will emit 50 tons of carbon emissions (Gu, Fan, Wu, Huang, & Jia, 2018). IT architects employed in small organizations with 100 or less users could reduce carbon emissions by 90%. Therefore, IT architects in an insurance company can contribute positively to social change by reducing carbon emissions.

A Review of the Professional and Academic Literature

The literature review conducted for this study includes information related to the research topic as well as analyses and syntheses of journal articles pertaining to cloud computing services and the TAM. In addition, background information is provided concerning cloud computing services along with the impact of cloud computing services from the perspective of business and IT resources. Also, I discuss the TAM conceptual framework. Although the constructs of TAM serve as predictors to the attitude of IT architects toward adopting new technology, the themes influence predictors such as PU and PEOU. During the review of literature, certain themes emerged which may impact an

IT architect's strategy when adopting cloud computing services. Themes such as such as security, privacy, and availability seemed common throughout the articles reviewed.

The purpose of this qualitative exploratory case study was to explore the strategies used by IT architects of an Illinois-based insurance company when making a decision to adopt cloud computing services. The goal of performing a literature review was to determine what strategies were used by IT architects as well as any themes impacting decisions to adopt cloud computing services. Despite features such as scalability, availability, agility, reliability, security, and pay per use pricing, some IT architects are still slow to adopt cloud computing services. The review of the professional and academic literature was instrumental in finding peer-reviewed articles appropriate for this study. During the search for sources, more than 250 sources were located, but after further review, 222 were used as references. Of the 222 sources, 206 or 94% were peer-reviewed and verified through Ulrich's Global Serials Directory and 196 or 89% were published within 5 years of my expected graduation date. Additionally, 104 of the 222 references were used in the literature review.

References used in this study were located using databases in the Walden University library. I set my oldest search year to 2013 and most recent search year to 2018 to stay within the five year requirement. Additionally, the databases used in the Walden University library were: ACM Digital Library, Computers and Applied Sciences Complete, IEEE Xplore Digital Library, Computing Database, ScienceDirect, ProQuest Central, and Academic Search Complete. Certain articles were found by using threads

from discussion questions and reading assignments in previous Walden University classes.

Impact of Cloud Computing Services

The benefits of cloud computing services are often looked at from the perspective of a company, but business objectives alone are considered a limited perspective. In order to obtain an understanding of the benefits of cloud computing services, different perspective such as business and IT resources must be considered (Mac-Anigboro & Usoro, 2015). The following sections will explore the benefits of cloud computing services from a business and IT perspective.

Business perspective. IT architects must account for the business perspective when deciding to adopt cloud computing services. The use of cloud computing services is viewed as business agility or the ability to rapidly deploy infrastructure through the efficiency of scaling IT resources (Oliveira et al., 2014). IT efficiency resulted from lower upfront costs, on demand access to IT resources, lower operating costs, scalability, and mobility (Mac-Anigboro & Usoro, 2015). With lower upfront costs, IT architects in companies can convert their IT resources from a capital to an operational expense. If the use of cloud computing services is embraced, the upfront cost issue is reduced or removed (Carcary, Doherty, Conway, & McLaughlin, 2014). Before an IT architect decides to adopt cloud computing services, all costs to transfer to a cloud solution are compared to staying on local hardware. Costs such as transferring remote business processes and increasing bandwidth to account for latency are accounted for in overall project costs (Ali, Soar, & Yong, 2016; Carcary et al., 2014). The cost benefit for IT

architects employed in small-to-medium enterprise (SME) is different from cost benefits of IT architects employed in larger firms.

IT architects employed in smaller organizations benefited from a public cloud versus IT architects employed in larger companies (Pakath, 2015). IT architects in smaller organizations achieved greater savings when dynamically scaling cloud computing services large enough to satisfy any foreseeable demand (Kaul et al., 2017). Private clouds are a better option for IT architects employed in larger companies because they are better suited to address service outages and security failure, and have enough resources to avoid a breach of contract (Pakath, 2015). Bildosola, Río-Belver, Cilleruelo, and Garechana (2015) determined that cost was the second biggest driving force behind cloud computing services adoption. The biggest driving forces for most IT architects were flexibility and the ability to scale IT resources such as databases and infrastructure at will.

The ability to scale IT resources up or down is simplified by using a centralized console for provisioning. The overhead to provision IT resources such as additional storage, network bandwidth, memory, and CPU is administered from a centralized management console. A centralized management console can lead to a faster solution implementation for many businesses (Wang et al., 2016). The traditional IT model is designed around the rule of IT architects paying for hardware to address peak processing, which means the same hardware may sit idle during nonpeak processing time. The adoption of cloud computing services will allow an IT architect to reliably scale IT resources up or down depending on business need and leads to a pay-per-use costing

model similar to utilities (Avram, 2014; Oliveira et al., 2014). In addition, the ability of an IT architect to reliably scale IT resources up or down may be viewed as PU or PEOU in the TAM intent to adopt cloud computing services.

IT architect perspective. Along with accounting for the business perspective, IT architects must account for their own bias towards adopting cloud computing services. Wu and Feng-Kwei (2015) noted that IT architects employed in larger enterprises may have to downsize their IT department or redefine IT roles, which could lead to job dissatisfaction. During an IT department redesign, 70% of IT resources roles will change to performing keep the lights on tasks instead of critical tasks (Willcocks, Venters, & Whitley, 2013). With the advent of cloud computing services, technical skills are more than likely to be outsourced than business-related skills. IT architects may want to increase their soft skills such as business understanding, relationship building, and focusing on strategy (Schneider & Sunyaev, 2016). Redefending roles and responsibilities are important when less IT resources are needed for critical tasks.

Reinvesting in the company is important when money is saved by adopting cloud computing services. Basahel, Yamin and Drijan (2016) indicated that 62% of IT architects chose to reinvest the money saved into the company. By reinvesting, IT leadership was able to increase headcount with other job functions and boost wages to drive product innovation. Increasing other job functions and reducing IT resources could pose a problem if a business process is moved back on-premise from a cloud service provider. IT resources with the necessary supporting skillset may no longer be employed in the company or there may not be enough resources to support the process once moved

back internally (Carcary et al., 2014; Olaronke & Oluwaseun, 2016). Furthermore, allowing IT architects to move from meaningless tasks to critical tasks such as business understanding, relationship building, and strategy may be viewed as PU or PEOU in the intent to adopt cloud computing services.

The impact of adopting cloud computing services was viewed from a business and IT resource perspective. The business perspective was viewed as the efficiency of scaling IT resources as needed. The ability to provision and scale IT resources as needed resulted in lower upfront and operating costs, scalability, and mobility. The IT resource perspective was a catalyst for business model transformation, and more importantly, the adoption of cloud computing services will change how IT architects view IT resources. IT architect roles and responsibilities could switch from keeping the lights on to focusing on strategy and building soft skills for relationship management. The business and IT resource perspectives are considered contributions to change, but more importantly, both could drive PU or PEOU in the intent to adopt cloud computing services.

Technology Acceptance Model

The TAM is a critical component of the literature review and will form the foundation of this study. Davis (1986) indicated a user's motivation to adopt a particular technology was explained by the following three factors: PEOU, PU, and attitude toward using (ATU) the technology (see Figure 1). PU is considered if a particular technology allows the user of said technology to increase their job performance through the use of the new adopted technology. PEOU is the user's perspective that the target technology is easy to use. Using the TAM also suggests PEOU influences PU because the easier the

technology is to use, the more useful the technology is deemed. Furthermore, the use of TAM proposes that PU or PEOU both influence a user's ATU of the technology as well as consistently explain 40% of a user's intention to accept and adopt a technology (Gangwar & Date, 2016). Researchers may use the TAM to explain a relationship between a user's technological acceptance and adoption and the technology's actual usage (Sharma, Al-Badi, Govindaluri, & Al-Kharusi, 2016). However, actual usage of the adopted technology was not considered in the original theory but was added in a later evolution.

Evolution of the theory. The TAM has evolved since it was proposed by Davis in 1986 due to increasing system failure and technology needs. IT professionals investigated different ways to determine a user's attitude toward adopting new technology. In the original concept for TAM, Davis' proposed system use was explained or predicted by user motivation. Davis later refined his model and proposed the motivation to adopt new technology explained by four factors: PEOU, PU, ATU the technology, and behavioral intention (BI) to use a new technology (Gangwar & Date, 2016). After Davis refined his model and proposed that PEOU had a direct influence on PU, Davis proposed PEOU and PU were influenced by system design characteristics represented as external factors. In 1996, Venkatesh and Davis removed ATU from the TAM because PU or PEOU were found to have a direct influence on the intent to use a new technology (Shiau & Chau, 2016).

Venkatesh and Davis understood the TAM was not without limitations and needed to address important factors such as external variables and social influence which

are beyond PU and PEOU in an intent to adopt new technology. In 2000, Venkatesh and Davis expanded the TAM theory to TAM 2 which includes external variables to account for the impact of social influence processes and cognitive instrumental processes on PU and BI (Budi & Rafur, 2017). The social influence processes consisted of subjective norm, voluntariness, and image. Additionally, the cognitive instrumental processes consisted of job relevance, output quality, result demonstrability, and PEOU. Venkatesh and Davis shifted the focus from PU and proposed determinants of PEOU to further understand how the perceptions of users change over time as the user obtains more experience with the new technology (Wook, Yusof, & Nazri, 2017). The new determinants TAM allows a researcher to focus on three main areas which are control, intrinsic motivation, and emotion as anchors for perceived enjoyment and objective usability. Although the TAM 2 addressed the lack of social influence in the TAM model, there were still other concerns still outstanding.

Venkatesh and Bala (2008) addressed the concerns of TAM 2 by proposing TAM 3 to explain individual user acceptance at a deeper level. In fact, Venkatesh and Bala proposed TAM 3 as a complete network of influencing factors related to compatibility, people, and usability of technology (Ganjikhah, Rabiee, Moghaddam, & Vahdat, 2017). Additionally, TAM 3 goes beyond TAM 2 by investigating voluntary and mandatory usage of technology over time. Just as TAM 2 tracks user perception over time, TAM 3 indicates that people pay more attention to the judgment about usability of a system based on the potential benefits obtained from social information shaping PU.

Supportive theories. During 1975 Fishbein and Ajzen conceived of the TRA to explain the adoption of new technology. Ajzen used the TRA as a basis to develop the theory of planned behavior (TPB) which uses behavior as an indicator to technology adoption. The TAM was a natural progression from the TRA and TPB because the use of TAM combined PEOU and PU as drivers toward BI and ultimately technology adoption (Shiau & Chau, 2016). The use of TRA indicates an individual's behavior is driven by their behavioral intentions and behavioral intentions are a function of an individual's behavior. The use of TRA defines intention as a direct determinant of behavior and is influenced by the attitude toward performing behavior as well as social pressures to perform a behavior (Sharma et al., 2016). The use of TPB indicates an individual behavior is dictated by an individual's attitude toward the behavior and subjective norms surround the performance of said behavior. The TPB is determined through the assessment of an individual's belief regarding consequences arising from their behavior and the ease with which the behavior can be performed (Lee, Li, Shin, & Kwon, 2016; Sharma et al., 2016). Therefore, the TAM is a natural progression from the TRA and TPB.

Davis was able to build upon the work started by Fishbein and Ajzen because the TRA and extended TPB both consider the use of a system as a behavior. Because of the behavior consideration, Davis accepted the TRA and extended TPB as suitable models, but changes were needed. To move forward with his conceptual model, Davis decided not to take the subjective norm into account when predicting the actual behavior of an individual. Davis also disregarded an individual's salient belief to determine attitude

toward a behavior, but identified two distinct beliefs known as perceived usefulness and perceived ease of use. The TRA and TPB were considered supporting theories to TAM, but contrasting theories to TAM were also researched.

Contrasting theories. The diffusion of innovation (DOI) theory was proposed by Everett Rogers in 1995 and has been used to explain how and when new technology is evaluated, adopted, or rejected by users. Rogers (2003) indicated perceived innovation attributes could influence acceptance of innovations. Perceived innovation attributes could explain 49% to 87% of new technology adoption, but only if the provided innovation idea is perceived as being better than the technology being replaced (Lee, 2016; Stieninger, Nedbal, Wetzlinger, Wagner, & Erskine, 2014). DOI contains five main attributes which are used to help explain innovation adoption in an organization and they are as follow: relative advantage, or the extent to which an innovation is better than the previous generation; compatibility, the degree to which an innovation can be assimilated into the existing business processes, practices, and value systems; complexity, how difficult it is to use the innovation; observability, the extent to which the innovation is visible to others; and trial ability (Oliveira et al., 2014). Stieninger et al. (2014) and Rogers (2003) indicated relative advantage is the most important factor of the five attributes when considering attributes pertaining to the adoption of new technology. DOI is considered as a valid contrasting theory to TAM, but the technology organization environment (TOE) can also be considered a contrasting theory.

The TOE framework was created by Rocco DePietro, Edith Wiarda, and Mitchell Fleischer in 1990 to examine the process by which IT architects adopt and implement

new technology. Some of the common technology attributes were derived from DOI (Lal, & Bharadwaj, 2016). Lian, Yen, and Wang (2014) indicated the adoption of technology is influenced by technological context, organizational context, and environmental context. Of the three factors indicated, the organizational context is higher than the environmental factor (Hsu, Ray, & Li-Hsieh, 2014). The organizational context is considered more vital as a combination of organization size, centralization, and the complexity of the management structure. The role of management adds gravity to the organizational context because top management establishes the climate for technology innovation and top management makes decisions on funding (Ray, 2016). Consequently, the support of management is needed to help adopt new technology concepts.

Criticism of the theory. TAM can be used to predict 40% of a user's intention to accept and adopt a technology, but not without limitations. One of the main limitations with TAM is self-reported data. Some Researchers argued that real use data is collected concerning technology usage by running reports on system usage versus feedback or information from individuals using the system (Shiau & Chau, 2016). Other researchers indicated TAM had restricted constructs and thus is not used to adopt newer services and solutions (Gangwar, & Date, 2016). A key construct to consider is whether system usage is mandated or not. Beyond self-reported data and restricted concepts, some researchers complained that TAM did not produce consistent or clear results unless significant factors were identified and included (Gangwar & Date, 2016). Without consistent and clear results, a research study may lose credibility explaining the intent to adopt new technology.

According to Gangwar and Date (2016), the appropriate theory to use as a conceptual framework depended on the research problem. While addressing the research problem, various themes must be taken into consideration. Security, complexity, regulatory compliance, strategy and other themes came to mind when an IT architect evaluates options to adopt cloud computing services. DOI explains how and when new technology is evaluated, adopted, or rejected by users, and TOE examined the process by which users adopt and implement new technology, but neither combine external factors with PU or PEOU. Gangwar and Date (2016) also explained external factors along with PU or PEOU in the TAM consistently explained 40% of a user's intention to accept and adopt a technology. Because TAM accommodates the use of external factors along with PU or PEOU to explain the motivation to adopt new technology, the use of TAM is ideal for this study.

TAM applied in other research. The use of TAM in research has crossed various disciplines such as the mobile phone industry, agriculture, healthcare, social media and education. Park, Im, and Noh (2016) used TAM to assess strategies affecting the intention to adopt LTE service in the mobile phone industry of South Korea. Almarashdeh and Alsmadi (2017) used TAM to gain insight into the development and acceptance strategies of mobile government services. Additionally, Hew, Leong, Tan, Lee, and Ooi (2018) utilized TAM to investigate a strategy for mobile social tourism in Malaysia. Pappa, Iliopoulos, and Massouras (2018) used the extended TAM 2 to investigate strategies influencing the acceptance and use of electronic-based traceability systems in agri-food chains. The broad use of TAM across multiple disciplines allow

researchers to explain an intention to accept and adopt a technology. Saeid, Yousef, Afsaneh, Mohammad, and Jahanpour (2018) utilized TAM 2 and TAM 3 to inform healthcare managers and policy makers that the quality of healthcare service could be improve using modern technology strategies. Furthermore, Huang (2017) used TAM to show that students with an awareness of others were influenced and motivated to use social media for collaboration and learning. Finally, Tripathi (2017) and Mark, Dietmar, Werner, Gerold, and Michael (2018) utilized TAM to understand strategies influencing the intention to use cloud computing services in an organization. TAM has been used by many researchers involving various strategies in the intent to adopt and use new technology such as cloud computing services, which is the purpose of this study.

Application of TAM in cloud computing services adoption. Many researchers have utilized TAM to study various strategies in the adoption of cloud computing services. Aharony (2015) found that behavioral intention to use cloud computing services was impacted by other TAM factors such as computer competence and personal characteristics which impacted PU and PEOU in the strategy to adopt. Additionally, the study highlighted the importance of individual traits such as cognitive appraisal, personal innovativeness, openness to experience and computer competence, when considering technology acceptance (Aharony, 2015). According to Aharony (2014), a strategy to adoption of cloud computing services is an individual experience and individual abilities play a key role in what is considered an impact to PU and PEOU in TAM. An individual that has a greater compute competency may find cloud computing services useful to their everyday job function. Furthermore, an individual open to new experiences will have a

different perspective concerning ease of use versus an induvial with less experience. However, the leaders or team of IT professionals seeking to adopt cloud computing services need to understand the impact of individual differences each person brings to the evaluation process when adopting cloud computing services.

In a study performed by Pedro, Francisco, and Mariano (2017), TAM was used to evaluate the adoption cloud computing services (SaaS) as a strategic technology. As a part of the study, external factors such as top management support, communication, organization size, training, and technological complexity were indemnified as strategies impacting PU or PEOU in the adoption of cloud computing services (SaaS). The original TAM explains about 40% of behavioral intent to use technology, but the five additional factors discovered during the research allowed the researchers to achieve 54.8% in behavioral intent to use cloud computing services (Gangwar & Date, 2016; Pedro, Francisco, & Mariano, 2017). During the research, a unique discovery was made impacting PEOU. All external factors except for training had an indirect impact on cloud computing services adoption via PU. However, training was the only external factor that impacted PU directly. Because of this discovery, the researchers suggested that PEOU is a better mediating factor than PU. In general PU or PEOU are used explained behavioral intent in the original TAM model, but external factors may have a direct or indirect effect on behavioral intent to use technology.

Several researchers have used TAM to explain the behavioral intent to adopt technology by using external factors influencing PU and PEOU. In the research conducted by Changchit and Chuchuen (2018), the external factors were not used to

influence PU or PEOU but were used to influence behavioral intent directly when adopting cloud computing services. The perceived cost of usage, perceived security, and perceived speed of access had a direct impact on behavioral intent to use in the adoption of cloud computing services (Changchit & Chuchuen, 2018; Pakath, 2015). Because Changchit and Chuchuen did not use the additional factors to drive PU or PEOU, cloud computing services were implied as being beneficial and useful. Additionally, PEOU was accepted as standard because the adoption of cloud computing services required less effort to support and was easier to use. However, the significance of this study is that TAM was used to show strategies such as implied perceived cost of usage, perceived security, and perceived speed of access had a direct impact on behavioral intent to use instead of impacting PU or PEOU and eventually behavioral intent.

TAM was also used to research under-investigated strategies of cloud computing services adoption such as expected benefits and perception of risk. Caldarelli, Ferri, and Maffei (2017) used an adapted version of TAM to address the concerns of expected benefits and perception of risk within a SME. Sandu, Gide, and Karim (2017) indicated that SMEs do not worry about extensive on-premise legacy systems which allows the emphasis on economic factors more than technical and organizational factors. The researchers were able to determine that SMEs were more likely to look past strong perceived risks to obtain high expected benefits. The significance of this study is that TAM was used to show SMEs are more likely to focus on economic gains impacting PU in the decision to adopt cloud computing services. Additionally, the study focused on the CEO point of view concerning the organization versus the view of the individual using

the technology. Furthermore, the study deviated from the normal TAM model by implying that perceived benefit was a better measuring attribute than PEOU.

The use of cloud computing services is not just for the corporate sector, but cloud computing services is a major part of education. Several researchers such as Lawrence and Tar (2018) used TAM to examine strategies to adoption of cloud computing services in the education field from a teacher perspective. However, Zeqiri, Aliu, Kostanica, and Prenaj (2017) study focused on the student perspective. Zeqiri et al. (2017) performed a study to research the adoption of cloud computing services but focused on software as a service (SaaS) and storage as a service (STaaS) as two separate models. The researchers used TAM but added a few external factors such as perceived risk/security, awareness, computer self-efficacy, and E-skills. Additionally, the students in the study used Dropbox and Google docs for storage and their cellphones as the primary device. The PU effect increased the odds of adopting SaaS by 2.220 times STaaS by 1.317 times (Zeqiri et al., 2017). The results of the study proved that PU impacted positively and directly towards a student's intent to use cloud computing services. However, PEOU was not considered significant in either model. In essence, the research indicated that students of today have higher E-skills and feel more comfortable with technology. Research indicates that comfort level with technology is what moved students beyond perceived ease of use and more toward perceived usefulness when adopting new technology. In a normal TAM construct, PEOU usually impacts PU because the easier the system is to use, the more useful the system.

The use of cloud computing services in the field of higher education is an ongoing journey and evaluation. Bhatiasevi and Naglis (2016) performed one of the first research studies focused on the use of cloud computing services in higher education. For the study, data was collected from two leading universities in Thailand (Mahidol University International College and Thammasat University). The significance of the study was the use of the original TAM construct. Some researchers create other perceived factors to drive behavioral intention and system use, however, Bhatiasevi and Naglis did not take that approach. The decision to use external factors such as subjective norm, perceived convenience, computer self-efficacy, trust and software functionality to impact PU or PEOU which in turn impacts behavioral intention and thus system use (Bhatiasevi & Naglis, 2016; Ho, Booth, & Ocasio-Velázquez, 2017). With the external factors and the original TAM construct, Bhatiasevi and Naglis were able to determine that perceived convenience and trust impacted PU. However, PEOU was impacted by computer self-efficacy and software functionality. An additional significance of this study is that TAM was used to show widespread adoption of cloud computing services within Thai users.

There were several studies performed concerning the adoption of cloud computing services in higher education but not many concerning a study performed after the adoption was made. Ashtari and Eydgahi (2017) utilized TAM to study PU and PEOU in higher learning after cloud computing services were adopted. Ashtari and Eydgahi hypothesized that the same construct used to adopt cloud computing services would remain important after the decision was made to adopt cloud computing services. Ashtari and Eydgahi focused on computer self-efficiency, internet self-efficiency, and

computer anxiety along with the normal PU and PEOU. Bhatiasevi and Naglis (2016) were able to use a similar external factor (computer self-efficacy) to drive PEOU in a previous study focused on the adoption of cloud computing services in higher education. Based on the data received in the study, Ashtari and Eydgahi were able to use TAM to show computer self-efficiency, internet self-efficiency, and computer anxiety still impact PU after cloud computing services were adopted.

Strategies Impacting the Adoption of Cloud Computing Services

TAM may be used in the decision to adopt cloud computing services. Various researchers including Gangwar and Date (2016) indicated TAM could be used to predict a user's intention to adopt certain technology based on PU and PEOU. The purpose of this qualitative exploratory case study is to explore strategies used by IT architects of an Illinois-based insurance company when making a decision to adopt cloud computing services. The TAM is used for exploration, but themes were discovered during the research of literature that impact strategies of adopting cloud computing services. During the literature review, themes such as availability, compatibility, complexity, compliance, confidentiality, implementation, integrity, portability, privacy, security, and trust were discovered. In this section of the literature review, I discuss various themes (strategies) influencing PU or PEOU in the TAM and ultimately impacting the adoption of cloud computing services.

Availability strategy. During the investigation of literature, availability emerged as a theme in the adoption cloud computing services. In fact, 29% of IT architects in a recent study listed availability as a key hindrance to adopting cloud computing services

(Ali et al., 2016). To help alleviate the issue of availability, IT architects can use strategies such as well written service level agreements, data availability, and effective networks.

An availability strategy may influence PU or PEOU in a decision to adopt cloud computing services. Phaphoom, Wang, Samuel, Helmer, and Abrahamsson (2015) explored cloud computing services as continuous availability and convenient access to business services and data. Availability to key resources is fundamental for a cloud service provider which leads to service level agreements encompassing service uptime and reliable performance (Dhasarathan, Thirumal, & Ponnurangam, 2017). However, some cloud service providers view availability based on service level agreements and uptime of their environments as the most important quality of measure when adopting cloud computing services (Phaphoom et al., 2015). Also, Zissis and Lekkas (2012) indicated a cloud service provider should have the ability to function even in the possibility of a security breach and especially during routine maintenance. Some IT architects indicated that availability issues could result from accidents during network or infrastructure upgrades as well as server patching. However, the most common issue related to availability is a large scaled service outage caused by an unexpected shutdown of virtual machines which ultimately impacts service level agreements (Phaphoom et al., 2015). Therefore, cloud service providers should have the ability to function regardless of a breach, routine maintenance or unexpected shutdown of machines.

To help minimize the impact of a large scaled service outage, researchers such as Okai, Uddin, Arshad, Alsaqour, and Shah (2014) proposed using different cloud service

providers for different purposes. As an example, Okai et al. (2014) determined Google cloud was a better solution for email services, but Microsoft Azure was better solution for platform as a service (PaaS) and infrastructure as a service (IaaS). The utilization of PaaS provides IT architects with a customized environment with different programming languages, operating systems, and databases (Sahdev, Medudula, & Sagar, 2014). IT architects using Microsoft's Azure were able to minimize hardware cost by providing disk pace and servers through virtualization in a dynamic cloud environment (Botta, de Donato, Persico, & Pescapé, 2016). Okai et al. (2014) also indicated the cost of splitting data is carefully considered depending on the pricing scheme of the supplier and needs of the IT architect. As cloud computing services advance, synchronizing data across different cloud service providers will become cost effective. The use of multiple cloud service providers is similar to the concept of using multiple network carriers to prevent outages if one network segment is compromised.

System assurance and availability is important in a strategy to adopt cloud computing services. Stallings and Brown (2014) stated availability is the assurance that systems will work promptly and access to services and data are not denied to authorized users when requested. The lack of data availability or inability of a cloud service provider to provide high availability architecture platform caused some IT architects to pause their move to cloud computing services (Bhattacherjee & Park, 2014; Soni, 2015). For example, availability to key services and data are critical, but data availability is more critical in some services which may lead to the loss of life. El-Gazzar, Hustad, and Olsen (2016) argued that the healthcare industry was such an industry and IT architects in the

healthcare industry cannot risk an adverse incident or down-time because lives may be lost if such an issue happened. However, an insurance company may consider their agency and claims systems are critical for daily operations. Without the agency system being online, a customer cannot obtain a quote or an agent cannot bind a policy for coverage. If the claims system is not available, a claims adjuster in the company cannot settle claims. Providing fast and reliable claims coverage during a loss is the primary function of an insurance company.

Data availability is a critical component in a strategy to adopt cloud computing services. To help overcome the issue with data availability, Gangwar and Date (2016) explored precautionary measures such as using a combination of on-premise storage and cloud backup provided by the cloud service provider. The use of on-premise storage and cloud storage provides redundancy, but now the customer has to maintain critical data in two different places which could lead to data sync issues. However, Okai et al. (2014) indicated customer data could move off-premise into two different data centers provided by the same cloud service provider. The two data center concept would remove unnecessary on-premise data storage and provide data availability and redundancy for the customer (Ye, Liu, Leung, & Chu, 2017). However, there is caveat to the two data center concept. Certain IT architects in organizations have limitations on whether their data can cross country borders or not. The ability to move data across country boundaries may have an impact on cloud computing services adoption as well as the use of the two data center concept to improve data availability (Gangwar & Date, 2016). Compliance and

legal restrictions require an IT architects to understand where data is stored during data center replication.

The use of an effective network is important in the adoption of cloud computing services. Ali et al. (2016) cited 81% of their research sample affirmed that the need of effective networks was an obstruction to availability as well as the adoption of cloud computing services. Based on interpretation of seminal sources, an effective network requires a powerful telecommunications backbone to prevent network latency or outages (Avram, 2014). Additionally, an effective network must have performance, reliability, and security (Ray, 2016). To mitigate the issue of availability through and effective network, IT architects and cloud service providers need to ensure their networks have redundant switches and uninterrupted power sources to keep their networks running through outages. However, the reliability of an effective network is measured by the frequency of network outages and the time it takes to recover from a network outage (Yang, & Lin, 2015). Additionally, Mohammed, Ibrahim, Nilashi, and Alzurqa (2016) indicated some IT architects in certain companies were attempting to deliver core solutions through cloud computing services, but implementation of an effective network limited their options. Without an effective network, the full potential of cloud computing services cannot be achieved. However, Avram (2014) indicated that implementing the best cloud computing services did not matter if the end user is not able to connect to the services offered. Mohammed et al. (2016) also indicated an effective network lead to higher costs and expenditures to provide internet connectivity in rural or regional areas leading to a barrier to adopt cloud computing services. Additionally, Avram (2014)

indicated that an effective network in rural and regional areas would provide advances in technology similar to advances provided by electricity. Furthermore, the full potential of cloud computing services depends on availability of effective networks for connectivity to said services.

In brief, availability in a strategy to adopt cloud computing services is viewed from different perspectives such as service level agreements, data availability, and effective networks. A well written service level agreement requires a cloud service provider to meet specific parameters concerning uptime of environments and applications leading to availability. Additionally, data availability as related to the inability of a cloud service provider to provide high availability architecture platform caused some IT architects to pause a migration to cloud computing services. Furthermore, IT architects view an effective network as a major component in the adoption of cloud computing services since cloud computing services are deemed always available. Finally, an ineffective availability strategy can influence PU or PEOU in a decision to adopt cloud computing services.

Compatibility strategy. During the literature review, compatibility emerged as another theme in the adoption cloud computing services. Compatibility is viewed as the ability to move on-premise or legacy systems to a cloud service provider. Not all applications or legacy systems are cloud ready which may cause integration issues when adopting cloud computing services (Pakath, 2015). To help with a compatibility strategy, IT architects can utilize hybrid cloud models, application programming interfaces (APIs), and extensible markup language (XML) (Abbas, Bilal, Zhang, & Khan, 2015). Without

the use of XMLs and APIs, IT architects do not have a way for legacy systems to move off-premise or integrate with cloud computing services.

Compatibility is a major theme influencing PU or PEOU in a decision to adopt cloud computing services (Sabi, Uzoka, Langmia, & Njeh, 2016). Phaphoom et al. (2015) indicated that compatibility issues were more prevalent when IT architects needed to integrate extensive workflows between a cloud service provider and on-premise systems. Furthermore, integration between two different systems and compatibility issue avoidance is achieved by utilizing a hybrid cloud solution which allows IT architects in an insurance company to integrate on-premise legacy systems with cloud computing services. Wu and Feng-Kwei (2015) predicted that hybrid cloud solutions would become the cloud solution of choice over public or private clouds. Additionally, hybrid cloud solutions are considered more feasible for large and multinational enterprise's (MNE) such as insurance companies. IT architects within large and MNE have the budget to spend on IT investments (hardware and software) required to maintain on-premise systems supporting mission critical applications and data. Mission critical applications and data will stay on-premise in private clouds or data centers and less critical applications can move to public clouds (Wu & Feng-Kwei, 2015). However, IT architects in small to midsized companies did not have to worry about extensive on-premise legacy systems which make the move to a public cloud solution easier (Sandu et al., 2017). Therefore, compatibility between on-premise and cloud hosted applications impact PU or PEOU in a decision to adopt cloud computing services.

The use of an API is pivotal in removing some compatibility themes in the adoption of cloud computing services. An API is typically used as an interface between two applications or programs, but in this case a cloud service provider and a legacy backend system. Opara-Martins, Sahandi, and Tian (2016) explored the process of using application programming interfaces to integrate cloud service providers with on-premise legacy systems to help eliminate compatibility issues. Instead of building a custom connection for each customer or legacy system, a cloud service provider can publish a standard set of APIs for integration. The standard APIs are usually REST APIs because REST APIs are robust yet utilize less bandwidth (López García, Fernández del Castillo, & Orviz Fernández, 2016). However, compatibility with various business systems is not usually straight forward and require extensive knowledge from IT architects in each of the internal departments. Each cloud services customer is responsible for understanding and maintaining their code needed to interact with APIs published by the cloud service provider (Saswade, Bharadi, & Zanzane, 2016). Gholami, Daneshgar, Low, and Beydoun (2016) indicated that customizing APIs to a particular cloud service provider is not recommended to prevent vendor lock-in. Because in doing so, a compatibility situation could occur if a cloud services customer decides to change their custom APIs.

The use of XMLs to transmit data is what makes strategies such as hybrid systems and APIs possible. Li and Wei (2014) indicated that XML is a flexible yet standard way to create an information format for electronically shared structured data via the internet or private networks. XML data is self-describing and self-defining, there is not a need to prebuild structure to receive and store data exchanged between a cloud service provider

and a cloud service customer. Because of the simple yet effective approach of using XMLs to transfer data, a cloud service provider can share information with multiple cloud services customers alleviating compatibility issues (Sun, Dong, Hussain, Hussain, & Chang, 2014). Therefore, the ability to exchange data between a cloud service provider and cloud service customer is critical in a decision to adopt cloud computing services.

In summation, the information reviewed during the literature process pointed to compatibility as a theme in a strategy to adopt cloud computing services. To help alleviate such themes, some IT architects utilized a hybrid cloud solution as well as APIs and XMLs. By utilizing a hybrid cloud solution, IT architects have the ability to integrate on-premise legacy systems with cloud computing services. Additionally, the hybrid solution concept will allow critical applications and data to stay on-premise in private clouds or data centers and less critical applications to move to public clouds. Furthermore, the use of standard REST APIs enables integration between a cloud service providers and customers with on-premise legacy systems. A cloud service provider can publish a standard setup of APIs to allow communication with multiple customers without additional custom connections. Finally, the use of XMLs contribute to availability strategies such as hybrid systems and APIs. An effective availability strategy may influence PU or PEOU in a decision to adopt cloud computing services.

Compliance strategy. Compliance was another theme that emerged during the literature review involving the adoption of cloud computing services. In addition, 17% of IT architects in a previous study indicated that regulatory compliance was a major concern when adopting cloud computing services (Tang & Liu, 2015). To mitigate

compliance themes, IT architects must implement a compliance strategy focused on areas such as the lack of industry compliance, regulatory compliance, data protection and location compliance. Sahdev et al. (2014) argued industry compliance was among the top five barriers preventing the adoption of cloud computing services. The lack of industry compliance caused many potential IT architects to steer clear of cloud computing services, but organizations such as National Institute of Standards and Technology and Cloud Security Alliance were formed in the late 2000s and instituted some regulations. Also, IT architects in the newly formed organizations educated the public as well as laid the foundation for rules to follow by customers of cloud computing services and cloud service providers (Raza, Adenola, Nafarieh, & Robertson, 2015). Additionally, the rules lead to the creation of user consent forms to deal with personal data, strong access mechanisms, compliance to data jurisdictions, and data confidentiality regulations (Grozev & Buyya, 2016; Phaphoom et al., 2015). Therefore, compliance is important in a strategy to adopt cloud computing services.

Regulatory compliance is considered one of the most important challenges of cloud computing services tied directly to data sensitivity and moves to the forefront when IT architects are considering adopting cloud computing services (Ohmann et al., 2015). Grozev and Buyya (2014) indicated that different levels of compliance are linked directly to customers using cloud computing services in business units such as banking and healthcare. IT architects operating in the public sector deal with sensitive data and therefore must comply with regulatory compliance of a country and an industry (El-Gazzar et al., 2016). In fact, an IT architect employed in the banking industry must

comply with Sarbanes-Oxley (SOX) and Payment Card Industry Data Security Standards (PCI-DSS). Moreover, an IT architect employed in the healthcare field must comply with Health Insurance Portability and Accountability Act (HIPAA) (Phaphoom et al., 2015). However, an IT architect employed in the insurance industry must comply with SOX, PCI-DSS, and HIPAA. IT systems in an insurance company may contain financial data, process credit card payments, and receive medical documents.

In addition to regulatory compliance, Ring (2015) argued data protection and data location were key in compliance because data protection is different for each customer of cloud computing services. Certain IT architects in organizations have limitations on whether their data can cross country borders or not. Furthermore, the ability to move data across country boundaries may have an impact on cloud computing services adoption as well as the cloud service provider chosen (Gangwar & Date, 2016). Grozev and Buyya (2016) explored scenarios when cloud data centers were located in geographically dispersed location. Certain customers of cloud computing services may have regulations indicating data must be stored in the home country of the organization. Because laws vary by country, the configuration of security policies to comply with all legal jurisdictions is extremely complicated (Ali, Khan, & Vasilakos, 2015). In Europe, there is a legal stipulation when transferring data to the US because European Union data stored in the US can become subpoenaed and included in E-discovery if a US company comes under investigation (Grozev & Buyya, 2016). Additionally, E-discovery may become a concern because a cloud service provider's hardware may be seized for an investigation and customer data would fall under the laws of the geographic location (Ali et al., 2015).

Data stored in a cloud service provider's data center is under direct control of the cloud service provider, but regulatory compliance is still the responsibility of the customer using cloud computing services (Novkovic & Korkut, 2017). Therefore, IT architects must have a clear understanding of how data is replicated and where data is stored.

To help address issues such as the lack of industry compliance, regulatory compliance, data protection and location compliance, IT architects should become familiar with the guidelines established by National Institute of Standards and Technology and Cloud Security Alliance. By researching established guidelines, IT architects will know what pitfalls to avoid when choosing a cloud service provider. Secondly, IT architects should inquire about data storage details and locations of data centers. Some cloud service providers have multiple data centers throughout the world to allow customers to choose the best data center satisfying regulatory compliance needs. By choosing the best data center location, IT architects can address data regulations laws and geographical locations issues that impact the compliance concern in the adoption strategy of cloud computing services (Dhasarathan et al., 2017). As shown above, an effective compliance strategy focused on industry compliance, regulatory compliance, data protection and location compliance may influence PU or PEOU in a decision to adopt cloud computing services.

Confidentiality strategy. Confidentiality was another theme that emerged during the literature review involving the adoption of cloud computing services. Confidentiality is also viewed as authorized parties or systems having access to protected systems and data (Zissis & Lekkas, 2012) framed. However, confidentiality encompasses more than

authorized parties or systems having access to protected systems and data. To help address confidentiality themes, IT architects should establish a confidentiality strategy focused on secure access protocols and establish procedures to audit a potential cloud service provider.

To ensure authorized parties had access to appropriate data, Okai et al. (2014) suggested a confidentiality strategy that uses digital or electronic signatures to authenticate the identity of the user seeking access or dissemination of confidential information. Also, Zissis and Lekkas (2012) expressed a cloud service provider's certified confidentiality strategy should not cause unnecessary confidentiality and privacy risks. In the insurance industry, confidentiality is required to ensure customer information is not exposed by implementing the appropriate protocols. Some cloud service providers may violate confidentiality protocols and guarantees by stating data is encrypted during transit as well as rest or claim data is replicated to a certain location (Okai et al., 2014; Wei, Ganjali, Beom Heyn, Sukwon, & Lie, 2015). Because data is the responsibility of the customer, IT architects must account for confidentiality when adopting cloud computing services.

Along with data confidentiality, IT architects must account for software confidentiality. Zissis and Lekkas (2012) indicated software confidentiality involved specific application or processes maintaining a user's personal data in a secure manner. When adopting cloud computing services, customers are required to delegate trust to applications provided by the cloud service provider. Cloud service providers must reassure potential customers that confidential data is safe by offering audit results when

requested (Olaronke, & Oluwaseun, 2016). In fact, Rasheed (2014) indicated confidentiality risks of cloud computing services adoption are always there regardless of the cloud model chosen (SaaS, PaaS, IaaS), but cloud service provider transparency and auditing would help because some cloud service providers do not allow customers to perform intrusion detection or encryption testing. In addition, audits are good for showing the impact of prevention and quality performance which gives context to security and defect responses (Coppolino, D'Antonio, Mazzeo, & Romano, 2017). Therefore, audits are important in a strategy to adopt cloud computing services.

In essence, confidentiality is another theme that emerged during the literature review with strategy implications to cloud computing services adoption. IT architects address confidentiality themes by establishing secure access protocols between their on-premise solution and the cloud service provider. Additionally, IT architects established audit procedures to validate confidentiality plans presented by cloud service providers. Giving potential cloud services customers access to audits may alleviate certain themes from customers thinking about confidentiality. Having an effective confidentiality strategy may influence PU or PEOU in a decision to adopt cloud computing services.

Implementation strategy. During the literature review, project implementation emerged as a theme in the adoption cloud computing services. Without a good project implementation strategy, IT architects are not able to clearly define a cloud computing services roadmap which may influence PU or PEOU. To help with project implementation concerns, IT architects can create an implementation strategy focused on a selection process, involve senior management and employees, and create a detailed

project plan.

Carcary et al. (2014) indicated that 48% of the participants listed a well-defined evaluation process to determine which IT services in their companies were appropriate to migrate to cloud computing services as a major concern. Additionally, Carcary et al. (2014) argued a poor selection process could lead to a costly and negative impact to the overall business strategy. Basic questions to adopt cloud computing services should influence strategic decisions and align with overall business objectives (Alkhuraiji, Liu, Oderanti, Annansingh, & Pan, 2014). Furthermore, El-Gazzar et al. (2016) indicated that the selection process needed to go beyond physical changes to infrastructure and consider more than the obvious technical issues, cost benefit analysis, and return on investment strategies. During the evaluation process, business processes undergo an identification, screening and categorization process to determine which processes are cloud ready now and which processes are not yet cloud ready (Carcary et al., 2014). Therefore, a well-defined evaluation process is important in an implementation strategy for adopting cloud computing services.

In addition to the evaluation process, Carcary et al. (2014) found that their study participants involved management, stakeholders, and employees in the cloud ready assessment. Senior management was considered one of the critical groups because senior management's attitude and perspective towards cloud computing services adoption was a direct correlation to positive influence on business operations (Lal, & Bharadwaj, 2016). The influence of senior management is important to ensure the IT resources needed to adopt cloud computing services are aligned to the overall business strategy (Hassan,

Nasir, Khairudin, & Adon, 2017). Furthermore, stakeholders were included in the adoption process to remove resistance to change in the implementation of new technology. Additionally, employees are a critical component because the more employees are aware and involved in the adoption process, the more employees will perceive cloud computing services as being easy to use (Carcary et al., 2014). Generally speaking, the influence of senior management in the implementation strategy to adopt cloud computing services is important.

Once a selection process is created and senior management is involved, a detailed project plan is created to prevent project failures and migration issues. Evidence in previous studies indicate that 30-40% of technology projects experienced cost overruns and 80-90% failed to meet performance expectations without a well written project plan (Yigitbasioglu, 2015). Wang et al. (2016) described employees, processes, and technology as three important elements to a successful project plan. Employees were listed because moving to cloud computing services changed the roles of employees. In fact, some employees moved from their old technical support roles to contract managers and IT resource planners. In addition, processes and technology were listed because processes, data, technology, and security moved from the secure confines of on-premise solutions to exposed vulnerable cloud solutions (Carcary et al., 2014). Wang et al. (2016) explained a successful project (cloud adoption) is performed in five distinct phases. The first step should begin with an assessment of cloud ready now processes planning to utilize the new technology. The second step is to provide training to employees at all levels to socialize change and remove and adversity to the new process. The third step is

to start small by moving noncritical processes first to make sure the solution is stable and build confidence in employee utilization. The fourth step is allowing your employees to settle into their new roles and responsibilities. The fifth and final step is repeating the process until critical processes are migrated to the cloud.

As shown above, an effective project implementation strategy is important in a decision to adopt cloud computing services. Project implementation concerns are addressed if IT architects create a selection process, involve senior management, and create a detailed project plan. Creating a selection process will allow IT architects to determine which business processes are cloud ready now and which process are not yet cloud ready. In addition to the selections process, involving senior management and employees in the strategy ensure resources needed to adopt cloud computing services are aligned to the overall business strategy. Finally, creating an effective implementation strategy is critical because an effective implementation strategy prevents project failures and migration issues which may influence PU or PEOU in a decision to adopt cloud computing services.

Integrity strategy. Integrity was another theme that emerged pertaining to the adoption of cloud computing services. Integrity is often viewed as protecting confidential data from unauthorized parties and guaranteeing the authenticity of the protected data (Zissis & Lekkas, 2012). To help mitigate an integrity circumstance, IT architects can implement an integrity strategy focused on data signing, whole file checking, encrypt data resting and inflight, and implement a software integrity check.

Data integrity is one of the key barriers which may influence a decision to adopt

cloud computing services (Oliveira et al., 2014). Also, data storage was one of the major uses for the adoption of cloud computing services, but the integrity of the data stored in the cloud was a key barrier to cloud computing services adoption. To increase data integrity, Piesse (2014) explored using a process known as keyless signature infrastructure (KSI) to sign data. KSI is a simple process of signing data by software whether the data is a policy or claim for an insurance company. KSI is considered the lie detector of data because verification is based solely on mathematics and not third-party software or cryptographic keys (Piesse, 2014). As an alternative to KSI, Chen and Lee (2014) proposed using whole file checking on stored data to increase data integrity. The method of whole file checking is to perform on data written and read daily, but archived data proved to be more complex. In contrast, long term archival data is usually written once and rarely read until needed. If data is accidentally corrupted or maliciously compromised, data corruption may be unknown until the data is recovered from cloud storage (Liu, 2013; Wei et al., 2014). Therefore, data integrity is important in the strategy to adopt cloud computing services.

Along with file checking, Okai et al. (2014) investigated encrypting data inflight as well as at rest. Coppolino et al. (2017) also recommended improving integrity by utilizing secure socket layer (SSL) and transport layer security (TLS) to prevent network sniffing and spoofing attacks. In addition to SSL and TLS, a key management system can prevent a man in the middle exploitation of data between the customer and the cloud service provider. The prevention of a man in the middle attack is important because the key selling point of cloud computing services is the ability to access uncompromised data

through a distributed method (Wei et al., 2015). Another method to ensure data integrity is to replace sensitive data with randomly generated tokenized data as well as a key management system to enforce authentication and authorization of data access. The above mentioned precautions can protect customer data to the edge of the cloud service provider, but cloud service providers must take additional steps to guarantee the integrity of customer data (Coppolino et al., 2017). Therefore, data encryption is important in an integrity strategy when adopting cloud computing services.

In addition to data integrity, software integrity was another factor impacting the strategy of IT architects adopting cloud computing services. Zissis and Lekkas (2012) argued that software integrity was the key component leading to data integrity. Software integrity should protect customer data from intentional or unintentional deletions, modification, theft or fabrication. Due to the lack of cloud computing standards, not all cloud service providers provide the same level of guarantee for integrity. To help ensure software integrity, Kouatli (2014) recommended cloud service providers use access control lists to prevent intentional or unintentional deletions. The access control list is setup for least privilege which means a user or application has enough access to perform a required function and no more.

Although the majority of software integrity protection is based on external threats, customers of cloud computing services face internal software integrity threats from other tenants or employees within the same cloud service provider (Stieninger et al., 2014). In fact, employees of cloud service providers may unintentionally become a threat by deleting important data or inadvertently corrupting data by mistake (Pakath, 2015).

However, E. Petac and A. Petac (2016) indicated the best defense against internal attacks is a good hypervisor. Multitenant cloud service providers understand the criticality of a good hypervisor because the hypervisor is the key to segmenting physical hardware into secure virtual hardware (Young, Lopez, Rice, Ramsey, & McTasney, 2016). Other tenants in the cloud may use cloud service provider resources to launch denial of service (DoS) attack against other tenants or external entities. To help prevent DoS attacks, Coppolino et al. (2017) recommended using filtration ingress or egress. Ingress filtering will prevent IP spoofing by dropping traffic from unknown domains. Egress filtering is an outbound filter that ensures only assigned or allocated IP addresses leave a network.

Given these points, integrity is a concern that impacts a decision to adopt cloud computing services. An IT architect can address integrity concerns by implementing a file checking process, encrypt data resting and inflight, and implement a software integrity check. The file checking process will validate if stored data has been compromised or corrupted before data is needed. Furthermore, proactive file validation will allow an IT architect to make additional backups before the data is permanently deleted. Additionally, encrypting data at rest and inflight will ensure the integrity of the data presented to each business system. Data is critical in the insurance industry because settlement of claims are based on evidence to prove fault. If the evidence or information is not trustworthy, denial of settlement and lawsuits could occur. Similarly, a software integrity check will allow IT architects to protect software from intentional or unintentional deletions, modification, theft or fabrication. Implementing an effective

integrity strategy may influence PU or PEOU in a decision to adopt cloud computing services.

Portability strategy. Portability was another theme that emerged during the literature review pertaining to the adoption of cloud computing services. Portability is viewed as the ability to move applications and data from one cloud service provider to another or between public and private clouds with minimal disruption (López García et al., 2016). To address the issue of portability, IT architects can implement a portability strategy utilizing application programming interfaces (APIs).

Proprietary add-on features presented by cloud service providers may impact portability. López García et al. (2016) determined that some cloud service providers attempted to attract customers by offering infrastructure and added value features. However, the added value features and services led to proprietary interfaces and eventually non-portability. However, cloud service providers are not bound by industry standards, each cloud service provider can create de-facto standards that may not be interoperable to other cloud service providers (Raza et al., 2015). In fact, non-portability is good for a cloud service provider, but non-portability limits availability, and interoperability for a customer seeking to adopt cloud computing services. With the limitation of portability, cloud service providers may inadvertently introduce uncertainty into cloud services adoption (Bhadauria, Chaki, Chaki, & Sanyal, 2014). Therefore, proprietary interfaces are not good for a portability strategy in the adoption of cloud computing services.

The use of APIs are critical in the adoption of cloud computing services. Phaphoom et al. (2015) felt the use of APIs could alleviate some problems of portability, but a cloud service provider may change APIs at any time. If an API is changed by the cloud service provider, a cloud service customer's ability to connect to the cloud service provider may become compromised or at worse lost. If a cloud service customer attempts to write a custom API, a cloud service provider could change connectivity protocols and access to cloud computing services would be impacted **(**López García, et al., 2016). Additionally, Pakath (2015) asserted API would not help if a cloud service provider were to go out of business. Kim (2015) noted a cloud service provider is usually bound by contract to give customers advanced notice of going out of business, an IT architect will have time to extract company data from the cloud service provider. If a cloud service provider does not give notice, valuable data will be lost unless the customer has a backup of company data.

In essence, APIs can help integration with a cloud service provider and alleviate some portability issues, but limited standards still may cause portability issues. Because of the limited standards and customized infrastructure, moving applications or data from one cloud computing service provider to another cloud service provider is complex (Dhasarathan et al., 2017). Therefore, the inability to move from one cloud service provider to another cloud service provider with ease is a theme influencing PU or PEOU in the adoption cloud computing services.

Privacy strategy. During the literature review, privacy emerged as another theme involving the adoption of cloud computing services. In fact, 49% of IT architects in a

previous study indicated privacy is their top concern (Tang, & Liu, 2015). To address the concern of privacy, IT architects must understand privacy laws and limit secondary usage of company data via structured contracts.

Privacy is deemed such a concern that IT architects perceive privacy as major concern in the adoption of cloud computing services. A. Ghorbel et al. (2017) indicated that organizations and individuals view data privacy as a major concern for their business. The impact of privacy in cloud computing can cause loses to a business that go well beyond finances and company reputation. Because of potential impact, IT architects must manage unauthorized secondary usage and trans-border data flow (Ali et al., 2016). In fact, unauthorized secondary usage by a cloud service provider was brought to the forefront with a lawsuit filed against Google. In the lawsuit against Google, the Swedish government indicated the contract provided by Google gives too much covert discretion over how user data may be used. In addition to naming a cloud service provider such as Google, a lawsuit could extend to subcontractors who fail to follow regulatory compliance for user data (Urquhart, Sailaja, & McAuley, 2018). Therefore, data privacy is important to IT architects when making a decision to adopt cloud computing services.

Information privacy laws are important in the adoption of cloud computing services. Gashami, Chang, Rho, and Park (2016) highlighted how information privacy laws intended to protect individual privacy were found to be inefficient when cloud computing services were being used. For example, Gashami et al. (2016) research focused on the limitations of trans-border data laws pertaining to data being shared by a cloud service provider and a subcontractor. However, the law did not apply to entities

such as Google because data was transferred from one department to another in the same business entity which is considered secondary use. In other words, IT architects in organizations face various requirements in an attempt to protect the privacy of customer information. When adopting cloud computing services, a customer's privacy policy must extend beyond on-premise confines to the cloud service provider. Privacy policies along with structured contracts must can account for unauthorized secondary usage and trans-border data flow (Dhasarathan et al., 2017; Yang & Lin, 2015). Hence, the need for IT architects to account for privacy laws in their strategy to adopt cloud computing services.

In short, an effective privacy strategy is considered an influencing of PU or PEOU in the adoption cloud computing services. IT architect address privacy concerns by understanding privacy laws and limiting secondary usage of company data. An effective way to limit secondary usage of company data is to write an effective structured contract stating what the cloud service provider is allowed to do with company data.

Security strategy. During the literature review, security of a cloud service provider emerged as a major theme in the adoption of cloud computing services. Customers of cloud service providers need to make sure their data is secure. Along with being secure, customers also need a guarantee that confidential data is not being accessed or used illegally by anyone including the cloud service provider (Rong, Nguyen, & Jaatun, 2013). To address the concern of security, IT architects must establish a security strategy focused on access controls, monitoring network attacks, establishing a secure cloud strategy, addressing internal and external attacks, writing a valid service level agreement, and addressing endpoint security.

Security is a major theme influencing the adoption of cloud computing services (Kouatli, 2014). Security is more than a technical problem encompassing application security, physical/technical equipment, but should include process and procedures for security guidelines (E. Petac & A. Petac, 2016). From a process and procedure point of view, an educational program must be implemented to teach personnel security best practices. Furthermore, security is a growing concern for on-premise or cloud based solutions because security threats and vulnerabilities continue to evolve as technology evolves (Ohmann et al., 2015). Ouahman (2014) suggested on-premise solutions are more at risk because on-premise infrastructure is consolidated in one place and security is limited by on staff security personal. IT architects may have limited security expertise, but a cloud service provider may have the ability to afford the best and brightest in cloud computing security. However, El-Gazzar et al. (2016) indicated that cloud computing services were more at risk because cloud computing services are exposed to diverse network attacks.

Exposure to diverse network attacks are common for cloud service providers. Ali et al. (2015) indicated network attacks were more prevalent because most cloud service providers use logical virtual networks running on physical networks. Virtual networks are used to communicate between virtual machines and virtual machines allow cloud service providers to maximize computing power on physical machines. Security professionals can use normal monitoring tools to detect intrusion on physical networks, but the same set of tools are not equipped to monitor virtual networks. Security professionals lose the ability to monitor for denial of services (DoS), spoofing and sniffing of virtual networks

when attempting to use normal physical network monitoring tools (Coppolino et al., 2017). To assist in monitoring virtual networks, a virtual security appliance may be encapsulated and dynamically deployed in the cloud infrastructure. Furthermore, a virtual security appliance has the ability to detect network traffic fluctuations and frequent network input/output that lead to performance and security issues (Lu et al., 2016). Because most cloud service providers offer multitenant solutions, network segmentations and security are important.

From a security perspective, a single security protocol or tool does not exist that can address all known and unknown security threats. In fact, one of the biggest barriers in security and monitoring is the use of familiar tools (Ali et al., 2015). Security professionals may choose to use a tool they are more familiar with but does not meet the necessary needs of the cloud service provider. The constant shift in security risks creates difficulty for security professionals and policy makers to perform an accurate threat assessment to deploy enhanced breach prevention (E. Petac & A. Petac, 2016). Ardagna, Asal, Damiani, and Quang Hieu (2015) explored the concept of using a secure cloud strategy. A secure cloud strategy focuses on identity management, access controls, trust management, and policy integration between multiple clouds. The secure cloud strategy also presents a security stack that builds on the following patterns: Gateway monitoring to limit surface attacks, monitoring for specific events, exchange of security tokens, and policy enforcement.

Cloud attacks can come from external sources, internal sources, and even the cloud service provider (Coppolino et al., 2017). External attacks on a cloud service

provider is usually leveraged against the cloud infrastructure via APIs and potentially insecure protocols across public networks (E. Petac & A. Petac, 2016). Such an attack could compromise security and impact data confidentiality and integrity. In contrast, internal attacks usually take place because the hypervisor separating virtual machines are easier to compromise internally than externally. Additionally, multitenant cloud service providers understand the criticality of a good hypervisor because the hypervisor is the key to segmenting physical hardware into secure virtual hardware (Young et al., 2016). A secure hypervisor is the key to maintaining all cloud service offering such as IaaS, PaaS and SaaS (Ali et al., 2015). In fact, multitenant cloud service providers face hypervisor threats more often than not because the attacker and victim could share the same host (E. Petac & A. Petac, 2016). Because most cloud service providers offer multitenant clouds using logical disks on a single infrastructure, data remanence may lead to the disclosure of data which cannot be mitigated by traditional security measures (Zissis & Lekkas, 2012). Coppolino et al. (2017) explored instances where employees from a cloud service provider exploited their privileges and stole sensitive data or manipulated the hardware platform of customers.

Due to the combined responsibility between cloud service providers and IT architects, contractual security via service level agreements must be agreed upon by each party (Wei et al., 2015). Typically, a cloud service provider will provide a service level agreement that governs performance levels such a reliability, availability, and more importantly security. In order to utilize infrastructure effectively and provide low cost services, cloud service provider may switch customer data and processes from one data

center to another causing privacy, security, and legal compliance concerns (Grozev & Buyya, 2016). Certain customers may want additional security guarantees restricting data storage to a certain geographical location or legal jurisdiction. To guarantee certain specifications and service level agreements are met; customers agree to pay fees for security guarantees, high availability, reliability, and security (Rehman, O. Hussain, & F. Hussain, 2015). Kouatli (2014) ascertained most cloud service providers will secure their own infrastructure, platforms, and applications, but customers must secure their own applications. Security vulnerabilities may shift to the cloud service provider, but customers must understand they are still responsible for customer data in infrastructure provided by cloud service providers. The underlying issue for customers was knowing where cloud service provider security obligations ended and where customer security obligations began. (Ali et al., 2016). Because cloud security may require obligations from the provider and customer, endpoint security for mobile devices could cause potentials issues for both parties.

The use of mobile devices allows a cloud service customer to extend the availability of an application or solution by pairing low cost energy efficient technology with cloud based applications. However, extending processing to mobile devices through cloud computing services comes with normal cloud security risks as well as endpoint security risks (Middleton, Scheepers, & Tuunainen, 2014; Ring, 2015). IT architects and cloud service providers must protect cloud solutions from various attack from the internet as well as entry points from mobile devices (Park & Kim, 2014). Mobile and cloud security becomes more complex when a user prefers to user their personal device instead

of a company issued device. Rubóczki and Rajnai (2015) explained the best way to close a security gap was to define a company policy pertaining to mobile device usage and utilize a mobile device management system. An effective mobile device usage policy must clearly define safeguards an individual user must accept only certain devices will be authorized for usage. The use of a mobile device management system will reinforce the mobile device usage policy by controlling mobile devices via security settings and certain confirmation for network connectivity, file synchronization, and encryption. Depending on the role and responsibility of an employee, file synchronization can be critical between mobile devices and the enterprise network (Ring, 2015). Certain employees must have real time encrypted data on their mobile device at all times. The use of a mobile device management system can control file synchronization as well as limit the ability of the user to download information to external devices or forward via email to nonapproved addresses. A mobile device management system can be configured to remote wipe a user's phone if lost to ensure company data is not compromised (Chang, Kuo, & Ramachandran, 2016). Therefore, real time data encryption and remote wipe capability is important for a mobile device management system.

Given the above information, a security strategy concerning cloud computing is important. An effective security strategy for cloud computing services may influence PU or PEOU. Security for cloud computing services is not one solution that covers all threats for various cloud computing customers. However, security is address by establishing access controls, monitoring network attacks, implementing a secure cloud strategy, addressing internal and external attacks, negotiating a service level agreement, and

addressing endpoint security. By addressing the above points, an IT architect can implement and effective strategy to adopt cloud computing services.

Trust strategy. Trust of a cloud service provider also emerged in the literature review. A trust strategy has the ability to influence PU or PEOU in a decision to adopt cloud computing services. IT architects can address a trust concern by establishing a good relationship with a cloud service provider and writing a clear and concise contract.

Trust between cloud service provider and cloud service customer is a critical factor influencing the adoption of cloud computing services (Ali et al., 2016). Customers located in public clouds are not as trusting as customers located in private clouds. The lack of trust is because public cloud customers are faced with external threats as well as internal threats (Wei et al., 2015). Besides, distrust between cloud service provider and customer can happen during the migration from on-premise to a cloud service provider because the customer is no longer providing physical or virtual security of the data (E. Petac & A. Petac, 2016). Gashami et al. (2016) indicated trust became more salient when an IT architect had a high level of uncertainty during the process of moving to a cloud service provider. To help prevent distrust, a cloud service provider should build a strong relationship with IT architects as well as write a clear and concise contract. The correlation between a cloud service provider's transparency and an IT architects' level of trust was considered significant enough to impact the strategy to adopt cloud computing services (Ohmann et al., 2015). Ali et al. (2015) also determined customers of public clouds learned to trust the cloud service provider to protect customer data based on transparency, but the same IT architects never trusted the other customers in the

multitenant public cloud. Trust is an important concern for IT architects and trust may influence the IT architect intent to adopt cloud computing services.

In essence, trust was another theme that emerged during the literature review. The lack of trust in a cloud service provider has the ability to impact the adoption of cloud computing services. As indicated above, an effective trust strategy is addressed by establishing a good working relationship with a cloud service provider and writing a clear and concise contract.

Transition and Summary

In this section of the proposal, I introduced the topic of cloud computing services. Additionally, I discussed the purpose of this exploratory case study was to determine the themes impacting strategies of IT architects adopting cloud computing services. Furthermore, I used the TAM as the conceptual framework to explore strategies impacting PE and PEOU in the intent to adopt new technology. Finally, I discussed a literature review concentrated on defining properties of cloud computing services, impact of cloud computing services, defining TAM and how it applied to this study.

In section 2, I expand on the study by focusing on key areas such as the researcher, participants, data collection, and validity. Additionally, the data collection section will cover the data collection instruments, data collection techniques, data organizational techniques, and data analysis techniques. Furthermore, I incorporate techniques to determine reliability and validity of the study.

In Section 3, I expand on the study by focusing on key areas such as the overview of the study, presentation of the findings, application to professional practice, and

implications for social change. Additionally, I include recommendations for action and further studies. Finally, I provide personal reflections for this study.

Section 2: The Project

In this section, I discuss key elements of the study such as the research method and design, data collection, reliability, and validity. The purpose statement is revisited along with background information regarding participants in the study. Additionally, I discuss data analysis which consists of data collection instruments and techniques as well as data analysis techniques. Reliability and validity of the study are also covered in this section.

Purpose Statement

The purpose of this qualitative exploratory case study was to explore the strategies used by IT architects of an Illinois-based insurance company when making a decision to adopt cloud computing services. The target population consisted of IT architects from an Illinois-based insurance company who have strategies to adopt cloud computing services. Each participant had a minimum of 5 years of experience in their respective field and the authority to impact decisions concerning cloud computing services adoption. The results of this study may provide other IT architects with valuable insight into specific strategies to improve their cloud computing services implementation. This study may contribute to social change by supporting the development of sustainable business models used to reduce infrastructure costs, increase flexibility, and improve business capability. Additionally, an implication of this study for positive social change is that IT architects in insurance companies can help reduce carbon emissions by using a multitenant cloud solution versus a brick and mortar data center.

Role of the Researcher

As the role of the researcher in this study, I work for the same Illinois-based insurance company, but in a different organizational structure. Because I am in a different organizational structure, I do not have the ability to impact a participant's environment from a professional or personal standpoint. To make sure I do not violate any protocols, I plan to use the Belmont Report as an ethical guide to protect the participants. The Belmont Report provides principles to ensure each participant receives respect, beneficence, and justice. As a researcher, I treated each participant with a certain level of respect by adhering to guidelines. Furthermore, I completed a web-based training course provided by the National Institutes of Health (NIH) and received a certificate for protecting human research participants .

As the researcher for this study, I have over 22 years of service with the company working in different aspects of IT. During my time with the company, I worked with claims adjusters, agents, and back office personnel supporting core business processes of the company. For the last eight years, I worked in the document capture industry first as a technical consultant and now as a manager of an application development and production support team. During this time as the senior leader, the application development and production support teams integrated our document capture platform with various back office systems to convert paper processes to electronic processes. The conversion to electronic documents allowed certain business units to move their workflow processes to centers outside of the United States, which reduced operating costs. In fact, integrating

with various backend systems gave me insight into the strategic vision of different business units and various struggles by IT architects adopting cloud computing services.

In conjunction with interview best practices and to help create a comfortable environment, I established a good rapport with each interviewee. Each question was semistructured and written in a conversational format. The conversational format allows participants to feel more at ease and allows each participant to speak more freely (Ajodhia-Andrews, 2016). In a qualitative study, the researcher is the main instrument for collecting and analyzing data, which may introduce bias. No matter how subtle the bias may seem, bias still may affect the study (Watson, 2015). Because I work for the same company being studied, personal predisposition and bias were accounted for in the study and mitigated. To help with the mitigation process, I remained open to new ideas and different perspectives. According to Castillo-Montoya (2016), using an interview protocol adds structure to the interview process, removes bias, and increase validity and reliability. As the researcher in this study, I adhered to a strict interview protocol to collect data adequately and prevent personal predisposition or bias.

Participants

The participants in this study consisted of IT architects with experience in developing strategies to adopt cloud computing services. The IT architects in this exploratory case study were from an insurance company based in Illinois. The criteria defined and used during the selection process for participants is crucial in qualitative research. Along with defining a selection process, Stern, Jordan, and McArthur (2014) indicated population and research questions are integral parts of developing participant

inclusion criteria. Each IT architect had a minimum of 5 years of experience in their respective areas such as security, architecture, business and systems analysis. Additionally, each IT architect had the authority to impact decisions concerning strategies for adopting cloud computing services for their respective business unit. The results of this study may provide other IT architects with valuable insight into specific strategies to improve their cloud computing services implementation. Information received from each participant may be used to contribute to social change and help other IT architects develop a sustainable business model used to reduce infrastructure costs, increase flexibility, and improve business capability.

Communication and engagement protocols are essential in a research study. Sharafizad (2016) indicated that researchers should follow a communication and engagement protocol before contact is made with potential study participants. If information is collected from a participant before consent is given, the collected information is not useable. Before a researcher can make contact with any potential participant, permission must be obtained from the insurance company's Corporate Relations Office (CRO). During communication with the CRO, the purpose of the study was explained in order to obtain permission to interview and record IT architects in the company. Each division of the company has different business objectives pertaining to cloud computing services, and therefore, information pertaining to the research was posted on an internal message board to allow random IT architects to apply. Once qualifications were validated, each participant was contacted via email with supporting documentation from Walden University introducing myself as a student and the nature of

my study. Techniques such as the use of informal language were used to help build a rapport with each participant. Each question asked in this study was presented in a semistructured format to emulate a normal conversation. The normal conversation technique put each participant at ease and allowed them to speak more freely. Additionally, participants who feel comfortable and speak freely are more likely to give truthful answers and not just the standard company boilerplate answer. Although I performed this study as a student of Walden University, I maintained a high level of professionalism and decorum per my company standards.

Research Method and Design

In this section, I focus on why the qualitative method was used as the methodology for this research study. The methodology, research design, population and sampling, and ethical research are discussed in this section. Additional information is provided to explain why quantitative and mixed methods were not suitable for this research study.

Method

Researchers use one of three methodologies for their research: qualitative, quantitative, and mixed methods. A qualitative methodology was used in this study because a qualitative methodology is primarily used to gain an understanding of underlying reasons, motivations and opinions contributing to a social or human problem. The purpose of using a qualitative methodology was to uncover the underlying reasons, motivations, and strategies used by IT architects when adopting cloud computing services. Additionally, the strategies of each research participants may be obtained by

methods such as observations and interviews (Cairney & St Denny, 2015). The use of observations during the interview process allowed me to watch the body language of the participant when they were answering the questions. Watching participant body language gave me insight into whether the participant was being honest or providing the boiler plate company answer.

The qualitative methodology utilizes inductive and deductive data analysis. Woiceshyn and Daellenbach (2018) indicated that inductive analysis allows a researcher to build patterns, themes, and categories from the bottom up and organize data into abstract units of information. However, deductive analysis also allows a researcher to look back at data from the view of emerging themes to determine if more evidence is needed to support the various themes. Qualitative methodology may start out as inductive, but a researcher may move towards deductive through process as analysis moves forward. Dowse et al. (2014) explored qualitative research as an emergent research design. Also, qualitative methodology is emergent because research is performed to learn about a problem or issue from the perspective of the participant. During the qualitative research process, a researcher must move beyond personal understanding of the problem and focus on the problem or issue through the eyes of the participant.

A quantitative methodology was considered, but ultimately was not used. A quantitative methodology was considered because a quantitative methodology is primarily used to quantify a problem by generating numerical data that is transformed into useable statistics for hypothesis testing. Furthermore, a quantitative methodology

allows a researcher to test specific hypothesis through a narrow scope under controlled conditions. Haegele and Hodge (2015) proposed that a researcher using quantitative methodology should adopt an objective stance and participants should provide anonymous responses via a survey questionnaire. Surveys in quantitative methodology are usually sent to large sample sizes that are randomly selected. Because I am doing an exploratory case study and my population size is small, a quantitative methodology was not chosen.

Deductive analysis of data is performed in both qualitative and quantitative methodology, but quantitative methodology accounts for specific variables being studied. Data is usually gathered and validated using data collection instruments such as surveys. In a quantitative methodology, the relationship between study variables is explained through data gathering and hypothesis testing. Researchers are able to test their variables using a confirmatory top down approach. Once data is collected from the survey instrument and analyzed using a statistical package, a statistical report is presented. The statistical report will provide critical information such as variable correlations, comparison of means, and significance of the findings (Durrani, Pita, & Richardson, 2014). Additionally, Durrani et al., (2014) indicated a quantitative methodology is deductive and has the potential to narrow the focus of studies. However, the goal of an exploratory case study is not to narrow the focus but to broaden in order to uncover as many themes as possible. Furthermore, a quantitative methodology was not chosen because a quantitative methodology has an objective stance and survey responses are anonymous. Data collection for this exploratory case study will consist of interviews

using semistructured questions to explore strategies used by IT architects to adopt cloud computing services.

A mixed methodology was considered for this study but was not chosen. A mixed methodology is a combination of both qualitative and quantitative which allows a research problem to be investigated from two different methods. The blending of methodology and data can provide a stronger understanding of the problem or question than one methodology (Almamy, Taina, Airi, Erkki, & Yue, 2015). Furthermore, a mixed methodology allows the use of semi structured questioning from qualitative methodology and closed ended questioning from quantitative methodology. Walsh (2015) examined the characteristics of mixed methodology and explained the methodology requires a researcher to perform adequate sampling, acquire enough source information, and complete all data analysis steps. Mixed methodology requires the collection of qualitative and quantitative data, but the data is analyzed separately and compared to see if findings match. During the collection and analysis of mixed method data, a researcher must be mindful and collect data in the correct sequence and determine if data from both methods require the same level of emphasis. In addition, the convergence or merging of data is the most challenging part for a researcher performing a mixed method study (Touray, Savolainen, Salminen, Sutinen, & Dai, 2015). Since this research study is not focusing on quantitative principles such as hypothesis testing and variable relationships, a mixed methodology was not chosen.

Research Design

Various design types are used in Qualitative research. The design types for qualitative research are case study, phenomenological, ethnography, and narrative analysis (Yilmaz, 2013). A case study design allows a researcher to analyze a person, events, decisions, or policies. In addition, a case study requires multiple sources of information such as interviews, participant observations, documents, and questionnaires (Yin, 2014). A case study design is proposed for this study to explore the strategies used by IT architects when adopting cloud computing services. Additionally, a case study design was used to explore strategies to reduce infrastructure costs, increase flexibility, and improve business capability.

A case study approach is useful when other researchers focus on developing a description and analysis of a case whether it is a single or multiple case (Yin, 2014). Moreover, case studies are useful when an understanding of specific case or cases is required. Robinson (2014) indicated the best unit of analysis for case studies is an event, program, or an activity with more than one participant. The case study design has many advantages such as challenging theoretical assumptions when studying uncommon phenomenon. Additionally, a case study allows a researcher to study a phenomenon without narrowing the focus of a study and provide context (Battleson, West, Kim, Ramesh, & Robinson, 2016). Furthermore, Battleson et al. (2016) explained that a case study is ideal to investigate contemporary phenomenon in real life context when the boundary between the phenomenon and the context is not clear. Furthermore, a case study is appropriate when a phenomenon is broad, complex, and the existing body of

knowledge is not enough to gain knowledge from casual questions. In a case study, a researcher can go beyond casual survey questions by conducting an interview and making observations during the interview to gain additional knowledge. The additional knowledge gained from facial expressions and body language can provide better understanding of the research problem. Therefore, a case study allows an in-depth holistic investigation to study a phenomenon outside of the context in which the phenomenon occurs (Rasouli, Trienekens, Kusters, & Grefen, 2016). Hence, the decision to use case study approach for this research.

However, case studies are not without disadvantages. Paulus, Lester, and Britt (2013) pointed out that case studies are hard to replicate, contained researcher bias, no classification because of small sample size, and are time intensive. Researcher bias is another issue in case studies because bias can take many forms such as subject bias, data collection, or the interpretation of data (Woiceshyn & Daellenbach, 2018). Another disadvantage is no classification because a small sample may limit a researcher's ability to generalize. The last disadvantage of a case study is time. The data collection process in a case study is very intensive and long especially if a researcher is not familiar with collecting and analyzing data for a case study (Paulus et al., 2013). Based on the above information, a case study may be difficult, but is still a valid option.

Phenomenological research is another design type used in qualitative research. A phenomenological research design seeks to understand the essence of an experience through perspective and perceptions of the event (Dixon, 2015). Dixon also explained that a phenomenological interview process is used to gather narrative material to help

understand the phenomenon being studied. Additionally, Moustakas (1994) explained a phenomenological research design focuses on lived experiences and perceptions to determine new knowledge from participants. According to Robinson, (2014), a researcher performing a phenomenological research study, must understand how social, cultural, and political aspects of the world shapes how a participant may answer a research question. Although certain aspects of the phenomenological research design were applicable for this study, most of the design was not appropriate therefore was not chosen.

Ethnography research is another design type used in qualitative research. Ethnography design was considered, but not utilized because ethnography design involves observations examining shared patterns of behavior, beliefs, and language in a cultural group (Thornham & Cruz, 2018). Ethnographic researchers obtain data based on personal observations, depicted events, and shared accounts concerning the culture of a group of people (Samnani & Singh, 2013). In fact, some researchers obtain data by immersing themselves in the everyday life and culture of the participants and such immersion requires an extensive amount of time. Muller, Mirza and Perret-Clermont (2016) noted time as a significant disadvantage during their ethnography research. Although access to the study participant's everyday life could be made available, access was not economically feasible nor would access to the participants everyday life added value to this particular study.

Other disadvantages to using ethnography were reliability, interviewer effect, inhibitions, and invasion of privacy. Ethnographers normally work along and would not have someone present to check their findings for reliability. Pallant, McIntyre, and

Stephens (2016) noted the disadvantage of not having someone to checking findings as inhibitions during data collection. Because Pallant et al. (2016) were playing a role that was not familiar to them as researchers, mistakes such as invasion of privacy could happen. Researchers using ethnography usually make observations and examine shared patterns. However, ethnography is not being used for this study due to limitations.

A narrative design was also reviewed for this study, but not chosen. A narrative design involves data collection from multiple sources to provide a detailed story of an individual or individuals. A narrative design or story telling may be used by a researcher to understand another person's life and giving the audience an opportunity to understand the experience of the participant (Palvia et al., 2018). Data may be collected through observations, documents, pictures, and other methods. Additionally, narrative research is often heard and shaped into a chronological order by a researcher (Dixon, 2015). Furthermore, Bell (2017) indicated a narrative design is best suited to understand the experiences of the participants. However, the goal of this study is to provide a focus on strategies used by IT architects when adopting cloud computing services.

The idea of data saturation in qualitative research is noted as being a contentious topic with diverse opinions. Researchers such as O'Reilly and Parker (2012) noted the concept of data saturation was originally developed with grounded theory in mind but was later adopted for other qualitative methods. Using the concept of data or thematic saturation, a researcher must add information from new participants until enough data is collected to replicate the study (Fusch & Ness, 2015). Additionally, a study reaches data saturation when additional collection of data does not contribute new data or themes to

the study (Yin, 2014). As the researcher of this study, I collected data until no new data or themes emerge. Furthermore, data saturation was achieved by using a purposeful sampling technique to collect data in the study population.

Purposeful sampling is another technique used by a researcher in a qualitative study. Using the purposeful sampling technique allows a researcher to select participants with knowledge and experience pertaining to the phenomenon being studied (Riungu-kalliosaari, Taipale, Smolander, & Richardson, 2016). Participants with extensive knowledge and experience with strategies to adopt cloud computing services are being interviewed to help with reaching data saturation. For this study, I am conducting semistructured face-to-face interviews to allow each participant an opportunity to answer the same questions. Van Horne and Murniati (2016) indicated the use of an interview protocol during the interview process will ensure the same questions are asked and no steps are missed in the process.

Population and Sampling

The target population for this study consisted of IT architects from an insurance company located in Illinois with multiple business units. The characteristics of the population in a qualitative study relates to the participants' subjective experience of the phenomenon being studied (Sharma et al., 2016). Dixon (2015) indicated performing a research study was more than choosing a methodology, writing interview questions, and picking a population to sample. Equally important, a researcher is required to know and understand the population being sampled. The first step in determining a sample size for a study is to determine the inclusion and exclusion criteria for participants (Robinson,

2014). If the first step of determining inclusions and exclusions is not followed, the research study may not have enough participants.

In a qualitative study, purposeful, quota, and snowball are three key sampling techniques. Purposeful sampling is widely used in qualitative research because purposeful sampling allows for the identification and selection of information-rich cases related to the phenomenon of interest. Additionally, purposeful sampling allows a researcher to select participants based on preselected criteria defined by the research question (Palinkas et al., 2015). However, some researchers think the use of purposeful sampling is judgmental and subjective since purposeful sampling is based on the characteristics of a population and the objective of the study (Park & Kim, 2014). Although purposeful sampling is considered judgmental, purposeful sampling is still considered a viable sampling technique for qualitative research design and this study.

Quota sampling is another technique used in qualitative research design. Quota sampling is a technique used by a researcher to ensure that key groups are represented in a sample. For example, a researcher could choose multiple groups and set a minimum of participants needed from each group. The quota sample is not set until each group is represented with the correct minimum number (Robinson, 2014). Finally, snowball sampling is another sampling technique used in qualitative research design. Snowball sampling is when current study participants refer future participants willing to participate in the study (Park & Kim, 2014). Additionally, snowball sampling is considered a nonprobability sampling technique because a researcher depends on participants to recruit future participants. Even though future participants are referred by current study

participants, a researcher must qualify each potential participant (Yigitbasioglu, 2015). For this study, I used a purposeful sampling technique to collect data from participants until saturation is determined.

Determining an adequate sample size to collect enough data is critical for a research study. Yin (2013) indicated that an ideal sample size for an exploratory case study is two to seven participants. For this study, I continued interviewing participants until the participants knowledge and experience with the phenomenon no longer provided new data or until all seven IT architects were interviewed. O'Reilly and Parker (2012) suggested there are various forms of saturation and the original form was theoretical saturation developed in the grounded theory approach. For data saturation in this study, saturation was viewed as thematic/data saturation meaning data collection took place via designated interview process until no new information was received from participants. In order to determine if no new themes have emerged, a researcher must analyze the data collected during the interview process to identify emerging themes. The process is repeated after each participant is interviewed to determine if new themes emerged. If a new theme emerges, a researcher must categorize the new theme and move forward with another participant. The entire process is repeated until no new data or theme emerges (Peng & Gala, 2014). The repetition of the process not only accounts for new themes, but ensure data saturation is achieved.

The site and setting of an interview are just as important to a researcher as choosing the questions being asked. As a part of interview process, a researcher must create a comfortable environment to establish trust and good rapport with each

participant. The conversational format allows participants to feel more at ease and allows each participant to speak freely (Ajodhia-Andrews, 2016). The interview setting is conducive for the interviewer as well as the interviewee. To help build trust and make the process conducive for each participant, the time of the interview is based on each participants schedule (Neuman, 2014). Additionally, a conference room located in the same building with the participant is utilized to avoid inconveniencing a participant. However, the location chosen must limit interruptions and avoid distractions that may affect data collection (Dowse et al., 2014). To limit interruptions for this study, a meeting room located in a low traffic area was utilized to minimize interruptions from individuals not involved in the study. Additionally, the meeting room being chosen was an internal meeting room with blinds which lessens the chance of distractions. Because the meeting room is internal and in a low traffic area, the setting minimized background noise which could have interfered with the recording of the interview (Peng & Gala, 2014). The meeting room was reserved 30 minutes before the first interview to allow time to remove any trash or unwanted items.

Ethical Research

Ethical research requires rules that each researcher should follow to protect research participants from harm. Researchers also have a moral duty to abide by certain principles and rules respecting the rights and dignity of each participant. Some of the rules are as follows: (a) informed consent, (b) withdrawal from a study, (c) protection of participants, (d) monetary incentive, and (e) confidentiality (American Psychological Association, 2002).

Along with guideline set forth by the American Psychological Association, I adhered to standards outlined by Walden University Institutional Review Board (IRB). Gergen, Josselson, and Freeman (2015) explained that IRBs evaluate risks, benefits, selection methods, informed consent processes, participant privacy and confidentiality involving research studies. Once my proposal was approved, I moved forward with the IRB process seeking approval to conduct research. Human subjects were used in my research therefore, IRB required each participant to give their consent voluntarily and freely via a written consent form (Oye, Sorensen, & Glasdam, (2016). Kornbluh (2015) indicated researchers should contact the IRB if unexpected issues arise or if a researcher needs guidance. As per IRB guidelines, I was required to contacted IRB if an issue arose and I was required to provide each participant with Walden University's contact information.

Consent in ethical research should go beyond a simple yes received from a participant. Before a researcher can begin a study, the detailed description of the study is provided to each participant on a consent form. As a part of the consent process, expectations for the researcher and participant are outlined. On the consent form, the benefits, risks, none use of incentives, and objectives of the study are clearly outlined so a participant can make an informed decision to participate or not. The consent form must also contain a statement explaining the study is voluntary and each participant has a right to refuse. In accordance to the Belmont Report, a participant can refuse to participate in the study at any time and there is not any consequences or loss of benefits (Hersh, 2014).

If a participant wishes to leave the study at any time, their wish is honored and noted on the consent form.

Protection of participants in a study is provided at all times according to the Belmont Report. In addition, a research study must not cause a participant unnecessary stress that would not occur in normal daily activities. Ajodhia-Andrews (2016) and Robinson (2014) indicated a researcher must protect vulnerable groups such as minors and the disabled. Since the group being interviewed in this study does not include participants from a protected vulnerable group, additional precautions to obtain signed consent forms from guardians is not required.

Additionally, privacy and confidentiality for participants is maintained throughout this study by not reveling participant names and keeping the research data secure. Johnson et al. (2013) explained that confidentiality is maintained throughout a study by using code names for each participant. The code book containing participant's true identities is stored on an encrypted USB drive. Also, the USB drive is being stored in a fireproof box for a minimum of 5 years. In addition to using code names for participants, code names are being used for business units to eliminate the possibility of someone cross referencing a participant's name with their business unit.

Data Collection

Data collections is considered one of the most critical steps in a research study. Data collection is a systematic approach utilized by a researcher to gather information concerning ideas, meanings, concepts, and phenomena to answer research questions (Elo et al., 2014). Data collection occurs by using various instruments and methods to obtain

information about the topic being studied. The next three sections will discuss data collection instruments, data collection techniques, and data organization techniques.

Instruments

There are various methods used to collect data in a qualitative study. The main methods of data collection techniques in qualitative research includes, interviews, participant observations, and document analysis (Melin & Axelsson, 2016). In this exploratory case study, I served as the primary instrument of data collection. In a qualitative study, a researcher serves as a nonbiased instrument that views study participants as experts. In addition to being nonbiased, a researcher is responsible for viewing information from various points of view yet maintaining consistency throughout the collection process (Neuman, 2014). Therefore, it is important for the researcher to stay nonbiased in order to maintain consistency.

Interviews. Interviewing is used to collect data in qualitative research. Peng and Gala (2014) indicated that conducting research interviews is one of the best ways to collect data in qualitative research. Additionally, Neuman (2014) indicated that semistructured interviews are designed to elicit participants' thoughts and ideas about the phenomenon being studied. Semistructured interviews are designed to focus the interview, yet leave questions opened ended. Open-ended responses allow additional probing to explore unexpected themes that emerge during the interview (Changthong, Manmart, & Vongprasert, 2014). Therefore, conducting interviews is an ideal approach to collect data for this qualitative research study.

To maintain consistency in the interview process, Van Horne and Murniati (2016) proposed using a guide called schedules or protocols designed to retrieve information from participants. For this study, I used an interview protocol to maintain consistency of the semistructured interviews. A copy of the interview protocol is included in Appendix A and a copy of the original interview questions are located in the Research Question section of this study. An interview protocol is used as a guide to guarantee pre-interview, interview, and post interview activities are performed consistently. Pre-interview activities consists of an introduction, verification of informed consent form, disclosure that the interview is recorded, and covering confidentiality. The main part of the interview process involved turning on the recording device, introducing the researcher, identify and stating the participants code stating the date and time, asking interview questions, asking for any additional information a participant would like to share, and stopping the recording. The post interview process involved explaining member checking to the participant, scheduling a follow-up meeting to validate data from member checking, thanking the participant, and providing the participant with my Walden University contact information.

Member checking. There are various ways to validate data and perform triangulation**.** Member checking as an element of triangulation involving feedback or respondent validation (Kornbluh, 2015). The technique is used by researchers to improve credibility, accuracy, validity, and reliability. Furthermore, Van Horne and Murniati (2016) indicated that member checking provides an opportunity for researchers to remove bias because each participant has an opportunity to review the accuracy of information

collected and transcribed by the researcher. Member checking is a repetitive process of analyzing and interpreting data looking for emerging themes from data collected from participants. The process of member checking will continue until the participant confirms all interpretations are correct, no additional clarification is needed, and no new information is added.

After each interview was completed, the recording of the interview was transcribed within 10 days and checked for accuracy. Sugihara, Fujinami, Jones, Kadowaki, and Ando (2015) indicated accurate transcription of collected information is critical to the reliability of information presented in a research study. To ensure accuracy of information collected during the interview process, I performed member checking within 10 days of the original interview. Before the meeting with each participant, I read and analyze the transcribed data looking for themes and understanding of the data. During the member checking session, I asked each participant to validate my interpretation and understanding of the information they provided during the interview process. I asked additional questions when necessary to seek clarity or understanding. As the last step of member checking, I asked each participant if they had additional data to share with me. If I received additional data, I determined if the additional data was new or part of an existing theme. I repeated the member checking process with each participant until no new data was collected.

To add additional context to information received during the interview process, Neuman (2014) suggested making observations and taking notes. Observations are the hallmark of many qualitative studies and occurs in layers. Initial observations are broadly

focused to allow researchers to learn about the participant's environment which may add context to the phenomenon under investigation (Changthong et al., 2014). The broader approach is then narrowed to help a researcher know what to focus on as the investigation continues. By performing transcription reviews in layers, a researcher can develop an appropriate level of understanding and form a perspective to analyze and interpret collected data (Kang & Stasko, 2014). Therefore, the use of semistructured interview questions and participant observation including notes should provide overall reliability and validity to this study.

Document analysis. Document analysis is another key step in qualitative research design. Document analysis includes written or recorded materials used to confirm events or provide explanations of certain data during a research study (Neuman, 2014). In case study research, document analysis is viewed as another source of data. The additional source of data is used by researchers to correlate information and addition additional context to collected data (Lub, 2015). Furthermore, Van Horne and Murniati 2016) indicated that additional data obtained from document analysis allows researchers to triangulate data to improve reliability and validity.

Data Collection Technique

To collect data in this research study, I utilized interviews and participant observations. However, before any recruitment of participants or interview of participants, approval from Walden University's IRB was obtained. The data collection technique involved obtaining consent from each participant, scheduling interviews, following an interview protocol, transcribing of data, and follow-up calls for member

checking. Van Horne and Murniati (2016) indicated an interview protocol is used to maintain consistency when interviewing each participant. As the researcher in this study, I used an interview protocol for consistency and a copy of the interview protocol is included in Appendix A. In addition, a copy of the original interview questions is located in the Research Question section of this study as well as Appendix D. Participants had adequate time to formulate their responses which also gave the researcher an opportunity to observe and collect field notes concerning body language.

Before an interview question was asked of any participant, the purpose of the study was explained to each participant. Along with the purpose of the study, a researcher must confirm the data collection process is understood by all parties involved. After each participant was briefed on the purpose of the investigation, a consent form was read to each participant to obtain permission to record the interview process (Sugihara et al., 2015). Peng and Gala (2014) stated interviews were typically used in qualitative research and were very effective in gathering and exploring human insight and perceptions of phenomena. During the interview process, a researcher often has an opportunity to probe beyond answers to predetermined questions. Probing beyond predetermined questions allows a researcher to seek further clarification or explanation certain responses (Sharafizad, 2016). However, probing beyond the predetermined questions may cause the participant to become uneasy.

In addition to interview questions, observation notes can improve an understanding of the information in the transcripts. Kang and Stasko (2014) suggested that observation notes are used to generate a rich understanding of the phenomenon being

studied. For a rich understanding in this study, observation notes were captured during the interview process to collect data concerning a participant's body language. The additional knowledge gained from facial expressions and body language can provide a researcher with a better understanding of a given research problem (Rasouli et al., 2016).

There are advantages and disadvantages of using semistructured interview questions and document analysis. Semistructured interviews are designed to elicit participants' thoughts and ideas about the phenomenon being studied. Semistructured interviews are designed to focus the interview, yet leave questions opened ended. Open-ended responses allow additional probing to explore unexpected themes that emerge during the interview (Changthong et al., 2014). A disadvantage to using semistructured interviews is increased travel cost, participants becoming disinterested or withdrawing from the study, participants not willing to answer truthfully for fear of company reprimand (Yin, 2014). Therefore, Skype may be used to help offset travel costs.

Document analysis is another key step in qualitative research design. The advantage is using document analysis is that written or recorded materials may be used to confirm events or provide explanations of certain data during a research study (Neuman, 2014). In case study research, document analysis is viewed as another source of data. The additional source of data is used by a researcher to correlate information and add context to collected data (Lub, 2015). Furthermore, the additional data obtained from document analysis allows a researcher to triangulate data to improve reliability and validity. The disadvantage of using document analysis is that company documents are sensitive and sharing with a researcher may go against company policy or the participant does not have

security clearance to remove documents from the company. For this research study, I used documents from the company intranet and SharePoint sites where access was provided. Document analysis was performed on company documents such as technology roadmaps, cloud initiatives for key business units, statement of works for current and future cloud solutions, and white papers.

After each interview was complete, the recording of the interview was transcribed within 10 days and checked for accuracy. To ensure accuracy, a transcribed copy of the interview was used to perform member checking and review before including the transcribed information in the analysis phase of a study (Sugihara et al., 2015). As a part of the member checking process, I scheduled a follow-up meeting with each participant to walk through the transcribed data. If data was not correct, I asked the participant to provide the correct information which I added to my notes. After I added the information to my notes, I reviewed the information to determine if the information was a new theme or if the information added clarity to existing information. Kornbluh (2015) described member checking as an element of triangulation involving feedback or respondent validation. The technique is used by researchers to improve credibility, accuracy, validity, and reliability. Furthermore, Van Horne and Murniati (2016) indicated that member checking provided an opportunity for researchers to remove bias because each participant has an opportunity to review the accuracy of information collected and transcribed by a researcher. Accurate transcription of collected information is critical to the reliability of information presented in the research study. Neuman (2014) explained a transcriptionist may remove extraneous comments from recordings, but a full record of

the interview is necessary to capture comments that may seem irrelevant. Because researchers read transcripts repeatedly to gain understanding, extraneous comments may lead to important results and conclusions.

Data Organization Techniques

Data organization is important in qualitative research. Elo et al. (2014) indicated that data organization is critical in understanding and analyzing collected data adding reliability and validity to a study. To help with data organization, a researcher should utilize codes and categories for sorting and comparing collected data (Kornbluh, 2015). Each participant in the study had an identifier code for tracking in the NVivo software to provide anonymity. The same participant code was used when creating folders to store participant's material such as recorded interview and transcribed interview statements.

Since each interview was recorded, a transcription of the recorded interview helped with analysis and allowed each participant to validate information collected during the interview. Each interview recording was transcribed and presented to the participant for member checking within 10 days to ensure accuracy of statements and transcription. Peng and Gala (2014) stated self-transcribing is important because self-transcribing allows a researcher to explore codes and identify emerging themes while carefully reading and rereading the transcriptions. The use of transcriptions also required additional protocols for coding and storage.

Researchers use different options to collect and code their information. For collection options in this research study, the NVivo software was used to code the transcribed recorded interviews. Additionally, Microsoft Excel was used to categorize

documents from the company intranet. Furthermore, the NVivo software allowed me to determine themes and subthemes from similar data in a specific dataset (Karanasios & Allen, 2014). Additionally, the NVivo software has an auto coding feature that is utilized if the transcribed information is in Microsoft Word, Libre Office Writer, or another word processing application with the ability to format data (Neuman, 2014). Because the use of recordings, participant observation notes, and NVivo software for coding, extra precaution is required to secure all information. All data such as recordings, participant observation notes, and the NVivo project file resides on an encrypted USB drive and stored in a locked fireproof box for a minimum of 5 years. All participant observation notes collected during the interview process were captured electronically on the interview protocol. In fact, capturing the participant observation notes via an electronic method allows storage on the same encrypted USB drive in the fireproof box. Johnson et al. (2013) explained converting and storing field notes electronically eliminate the need to keep additional paper. All paper (not converted to electronic) and electronic copies of data will be kept in a locked fireproof box for a minimum of 5 years before being destroyed. The drive will be over written and reformatted several times to remove as much readable data blocks as possible before destroying. Paper copies of information will be shredded in a cross-cut shredder to eliminate identifiable information from becoming discernible.

Data Analysis Technique

In this section of the study, I will cover the data analysis technique used to analyze data collected concerning organizational strategies and policies for the adoption

of cloud computing services. Data analysis is a process that seeks to understand the meaning of data by collecting and grouping information to categories (Bengtsson, 2016). In a qualitative study, data analysis is performed from an inductive and deductive point of view (Cohen et al., 2015). Additionally, inductive analysis utilized a bottom up approach to organize data in to abstract unit of data to build patterns, themes, and categories (Bengtsson, 2016). Along with the interview questions and answers, the primary research question is included in NVivo. A copy of the original interview questions is located in the Research Question section of this study as well as Appendix D.

The analysis technique chosen for this study is the thematic analysis technique. Peng and Gala (2014) stated the thematic analysis technique is one of the predominant techniques used in qualitative studies. The thematic approach requires a researcher to carefully read and reread transcribed data searching for identifiable codes and themes important to the phenomenon being studied. The approach also requires a researcher to review participant observation notes for information captured concerning a participant's surroundings and body language. All of information must be analyzed to determine themes and subthemes in the data (Castleberry & Nolen, 2018). To effectively utilize the thematic approach, Gan and Balakrishnan (2014) explained that thematic analysis is performed in six distinct steps. The steps or phases are as follows: Familiarization with data, generating initial codes, searching for themes among codes, reviewing themes, defining and naming themes, and producing the final report. Additionally, Alfaro and Watson-Manheim (2015) explained that coding is done line by line to allow themes to emerge from the collected data.

The first step requires a researcher to read and reread data to become familiar with intricacies and paying attention to emerging patterns. Along with reading and rereading the data, notes are being taken to track ideas and the coding process. The use of notes will allow a reflection on the analysis of the data and refer back to previous ideas as needed. The outcome from the first step is preliminary start codes and high-level themes.

The second step requires a researcher to generate initial codes and document how and where patterns occur. Karanasios and Allen (2014) explained a researcher should not have preconceived biases for patterns, but let the patterns emerge naturally. During the coding process, multiple coding methods are being used to generate the list of initial codes that represent the data collected from each research question. Additionally, thoughts and ideas concerning the initial code is logged in my notes. The results of second step is a detailed list of codes explaining how data answers the research question.

The third step requires combining codes into overarching themes to accurately depict the research data. Multiple cycles of reading and coding will take place to look for emerging, themes, subthemes, patterns and relationships in the data. Furthermore, the themes and subthemes are categorized and organized into different spheres of knowledge. The process is repeated as necessary to ensure meaningful explanations of the phenomena aligned with the research questions. The expected outcome of the third step is a list of sub themes for further analysis.

The fourth step requires a researcher to understand how data supports the themes and the overall theoretical design. Since TAM was proposed for this study, each theme and subtheme are checked for influence to PU and PEOU. Because PU and PEOU in

TAM indicates a user's intent to adopt new technology, patterns and themes should emerge to support the influence. The result of the fourth step should explain how patterns and themes tell a story about the data.

The fifth step requires a researcher to define each theme, what aspect of the data is captured, and what makes each theme interesting. Additionally, the fifth step should explain which themes contribute to understanding the data. Finally, step six is when a researcher writes the report (Gan & Balakrishnan, 2014). Furthermore, step six is considered the culmination of the researcher efforts and understanding of the research project.

Qualitative data analysis requires a researcher to utilize multiple types of data looking for emerging patterns. Cohen et al., (2015) indicated that qualitative methodology utilizes inductive and deductive data analysis to identify patterns in data. For analysis in this study, the NVivo software was used to code the transcribed recorded interviews. Microsoft Excel was used to categories documents from the company's intranet. The NVivo software allows a researcher to determine themes and subthemes from similar data in a specific dataset (Karanasios & Allen, 2014). Additionally, the NVivo software has an auto coding feature that is utilized if the transcribed information is in Microsoft Word, Libre Office Writer, or another word processing application with the ability to format data (Neuman, 2014). The advance features of NVivo allows a researcher to visualize data through the use of models, graphs, reports, and maps to uncover emerging themes (Paulus et al., 2013). Because of the advanced features of the NVivo software, NVivo is utilized to generate word trees, mind maps, and graph to add

visualization to the data. The additional visualization of the data will simplify the task of interpreting the data and confirming when no new themes emerge for data saturation. Along with the use of the NVivo software, data was sorted and analyzed multiple times looking for themes ore subtheme that may influence PU or PEOU of TAM.

Relevant information pertaining to the research topic is included in the data analysis. Along with information concerning the research topic, additional information is added based on relevancy of the research questions and data impacting PU or PEOU in the TAM conceptual model. Additionally, new studies pertaining to the adoption of cloud computing services were added.

Reliability and Validity

Reliability and validity are key components of qualitative research. In qualitative research, the findings of a researcher must be credible and repeatable for other researchers to deem the information reliable (Lub, 2015). In quantitative research; reliability and validity are viewed separately. However, researchers performing qualitative research view reliability and validity in terms such as credibility, transferability, and trustworthiness. In fact, reliability is often referred as the repeatability of findings if research is conducted a second time. Validity refers to the believability or credibility of research finding (Golafshani, 2003). Hence the important of reliability and validity in qualitative research to help establish research creditability.

Dependability

Dependability is important in qualitative research. Golafshani (2003) indicated that dependability in qualitative research begins with consistency in the method used to

collect data. Additionally, Peng and Gala (2014) indicated that dependability is more about a researcher using the same method or instrument to recreate a study more than once. According to Castillo-Montoya (2016), utilizing an interview protocol will add structure to the interview process, remove bias, and increase dependability concerning the strategies to adopt cloud computing services. As the researcher in this study, I adhered to the interview protocol to prevent predisposition or bias in order to obtain dependable, qualitative data.

Collecting insightful and dependable data concerning the adoption of cloud computing services depends on the answers provided by IT architects participating in the study. To increase dependability in qualitative research, Kang and Stasko (2014) suggested using observation notes to generate a rich understanding of the phenomenon being studied. For a rich understanding this study, observation notes are captured during the interview process to collect data concerning a participant's body language. The additional knowledge gained from facial expressions and body language can provide a researcher with a better understanding of a given research problem (Rasouli et al., 2016). Therefore, observation notes are important to provide additional information that interview questions alone cannot provide.

Credibility

Credibility is another important concept in qualitative research. Credibility in research is important because reliability determines how a researcher can persuade their audience that the research performed if worth trusting (Golafshani, 2003). Credibility in qualitative research is viewed differently than credibility in quantitative research, but

both require reliability. Because quantitative researchers attempt to disassociate themselves from the research process as much as possible, bias is less of a concern. However, bias is a major concern for qualitative researchers because qualitative researchers embrace their role and involvement in the research process. Unfortunately, bias may lead to credibility issues with research studies because the researcher is a data collection instrument (Golafshani, 2003). To overcome bias in a qualitative study, a researcher must first admit certain biases and assumptions exist. To help with the bias issue, a researcher can validate information by presenting transcribed interview notes to each participant for review. Each participant will have an opportunity to confirm if information captured and transcribed during the data collection process is accurate or not. If the collected information is not accurate, the participant can discuss necessary corrections with a researcher. Once all corrections are made, a corrected copy is sent to each participant to confirm all corrections were made (Van Horne & Murniati, 2016). Sharafizad (2016) indicated the use of multiple interview participants, observations notes, and policy documentation can help minimize bias and improve credibility of the study. Because data in this study is collected from each participant, there is an opportunity to cross analyzed data leading to increased credibility.

Methodological Triangulation is another way a researcher can make use of multiple sources of data and methods to provide corroborating evidence (Shamala, Ahmad, Zolait, & bin Sahib, 2015). Larosiliere and Carter (2016) proposed using multiple techniques to capture secondary data for triangulation to increase validity in research studies. Additionally, Yin (2014) considered multiple participants as multiple

data sources. Triangulation in this study is accomplished by using semistructured questions as the primary method of data collection and documents presented from the company as the secondary method of data collection. Additionally, the third method of data collection may utilize organizational strategies and policy documentation to help with triangulation of data received during the interview process (Lub, 2015). By cross referencing both sets of data, a researcher may be able to tell if a participant is uncomfortable answering a question. If the participant is uncomfortable or shows certain body language, the participant may answer the question untruthfully (Laumer, Maier, Eckhardt, & Weitzel, 2016). Unlike quantitative studies where triangulation causes disconfirmation in hypothesis, Golafshani (2003) indicated qualitative studies benefit from triangulation because convergence of data from multiple sources forms themes or categories for the study.

Transferability

Transferability in qualitative research is important. Neuman (2014) indicated that transferability in qualitative research is the degree to which findings from one study is applied in another setting. A researcher must provide as much detail concerning the context of the phenomena being studied to enable transferability to different settings (Golafshani, 2003). Robinson (2014) indicated transferability may be achieved if detailed information concerning participants, sampling, population, and results are provided to future researchers. However, it is up a researcher from different settings to determine if the findings are relevant for their setting. In this study, I provided detailed information to ensure transferability.

Confirmability

In qualitative research, the concept of confirmability is described as a broad term. Golafshani (2003) indicated confirmability is affected by a researcher's perception of validity in a study. Researchers may develop certain concepts of validity based on terms such as rigor, quality, and trustworthiness. In qualitative studies, new concepts of trustworthiness have replaced reliability and validity in certain instances (Sharif, Troshani, & Davidson, 2015). Researchers are faced with testing validity using reliability, but the test is usually overcome by using triangulation for testing and controlling bias (Sharif et al., 2015). Other techniques used to improve reliability and validity are peer review and external audit. Mazerolle, Burton, and Cotrufo (2015) indicated peer reviewers are individuals who keep researchers honest by performing an external check of the research process. Similar to peer review, external audits are performed by external consultants that examine both process and product of the research assessing study accuracy. Unlike a peer reviewer, an external auditor does not have any connection to the study (Bell, 2017; Lub, 2015). Therefore, confirmability is important in qualitative research.

Data Saturation

The idea of data saturation in qualitative research is noted as being a contentious topic with diverse opinions. Researchers such as O'Reilly and Parker (2012) noted the concept of data saturation was originally developed with grounded theory in mind but was later adopted for other qualitative methods. Using the concept of data or thematic saturation, a researcher must add information from new participants until enough data is

collected to replicate the study (Fusch & Ness, 2015). Additionally, a study reaches data saturation when additional collection of data does not contribute new data or themes to the study (Yin, 2014). As the researcher in this study, I collected data until no new data or themes emerge.

Transition and Summary

In this section of the proposal, I covered the methodology being used to conduct this study. Additionally, I included the role of the researcher, participants, research method and design, data collection, reliability, and validity. Also, I covered data collection instruments, data collection techniques, and data analysis techniques. Finally, I covered dependability, credibility, transferability, confirmability, and data saturation in this section.

In Section 3, I expand on the study by focusing on key areas such as the overview of the study, presentation of the findings, application to professional practice, and implications for social change. Additionally, I include recommendations for action and further studies. Finally, I provide personal reflections for this study.

Section 3: Application to Professional Practice and Implications for Change

The focus of this study was to explore strategies used by IT architects of an Illinois-based insurance company when adopting cloud computing services. In this section, I explorer these findings from individuals in the profession. This section includes (a) an overview of the study, (b) presentation of findings, (c) application to professional practice, (d) implications for social change, (e) recommendations for action, (f) further study suggestions, and (g) personal reflections and a conclusion.

Overview of Study

The purpose of this qualitative exploratory case study was to explore the strategies used by IT architects of an Illinois-based insurance company when adopting cloud computing services. The data came from interviews conducted with IT architects from various business units within the company. Additionally, the interviews were conducted in an environment which allowed each participant to feel comfortable and provide detailed responses to the seven semistructured interview questions (see Appendix D). The findings showed methods, strategies, and considerations used by IT architects when considering the adoption of cloud computing services for their respective business unit.

Presentation of the Findings

This section contains a discussion of the four themes that emerged during the study. The purpose of the study was to answer the research question: What strategies do IT architects of an Illinois-based insurance company use to adopt cloud computing services? The answer to this question may be used to help other IT architects develop a

sustainable business model used to reduce infrastructure costs, increase flexibility, and improve business capability. Semistructured interviews were conducted to gain an understanding of strategies used by IT architects to adopt cloud computing services. Additionally, purposeful sampling was used to collect data from seven participants during the interview process. In addition to semistructured interviews, company documents were reviewed for information concerning strategies used to adopt cloud computing services. Furthermore, access to company documents allowed for triangulation and validation of information obtained during the interview process. All interviews were conducted in a distraction-free conference room and did not last more than 60 minutes.

The six-step thematic analysis process served as the approach used for data analysis of collected data. After transcribing the interviews from all seven participants, the transcriptions were imported into NVivo 12 software for analysis and coding. Microsoft Excel was used to categorize documents reviewed from the company intranet. Using NVivo 12 software and Microsoft Excel helped me identify 13 core emergent themes and the frequency of each theme. Furthermore, the 13 core emergent themes were categorized into 4 primary themes based on commonalities. The four primary themes were as follows: (a) strategies to adopt cloud computing services, (b) strategies to adopt cloud services models, (c) strategies to adopt cloud computing models, and (d) concerns affecting strategies to adopt cloud computing services.

For this exploratory case study, the TAM conceptual framework was used to examine strategies used by IT architects when adopting cloud computing services. The TAM framework can examine an individual’s intention to adopt new technology based

on PU or PEOU. Additionally, my examination of interview transcripts from each participant and review of company documents allowed me to determine if PU or PEOU exist.

Theme 1: Strategies to Adopt Cloud Computing Services

Strategies to adopt cloud computing services was one of the themes that emerged from the interviews and supporting documents. The strategies consisted of the company directive, Twelve-Factor application methodology, and Six "R" approach which aligned with various components of the implementation strategy in the literature review. Creating strategies to adopt cloud computing services is critical because effective strategies prevent project failures and migration issues which may impact a company's ability to successfully adopt cloud computing services.

Company directive. Company directive was a theme that emerged during data analysis and aligns with the implementation strategy in the literature review. Company directive aligns with senior management attitude and perspective of an implementation strategy. Establishing a clear company directive and obtaining support from key stakeholders and senior management is important to adopt cloud computing services (Garrison, Rebman, & Kim, 2018). IT architects, key stakeholders, and senior management must align concerning objectives and guidelines for the company to follow when adopting cloud computing services. IT architects must understand the key business initiatives of their respective business units to determine how the business initiatives may be met while staying within the company directive. Therefore, IT architects must

understand which cloud services models and cloud computing models will provide viable options for their respective business units.

Company directive was a theme that each participant discussed and noted was important. Eleven company documents supported company directive as a theme (see Table 1). Participants 1, 2, 3, 4, 5, 6, and 7 indicated that a company directive was important when adopting cloud computing services. Participant 3 indicated the key to having a successful company directive was having senior management support and endorsement. Participant 3 noted that "without senior management endorsement, business units and other IT architects are not likely to embrace the company directive to adopt cloud computing services". A clear company directive supported by senior management will prevent the opt-out mindset. Also, having senior management support will help align key stakeholders in other business units being impacted by decisions to adopt cloud computing services.

Table 1

Themes for Strategies to Adopt Cloud Computing Services

	Participant		Document	
Theme	Count	References	Count	References
Company Directive	7	37	11	23
Twelve-Factor Application Methodology	6	17	5	13
Six "R" Approach	6	23	5	13

Analysis of the technology communication document indicated the company's directive is to move 70% or more of the current applications to the cloud within the next

three to five years. Moving more applications to the cloud allows IT architects to reduce application total cost of ownership (TCO). TCO calculations are generally made to compare cloud-based infrastructures with in-house infrastructures and SaaS models with on-premise software (Giray & Tüzün, 2018). Company documents defined TCO as technical debt from application development and production support. However, to accurately account for TCO, IT architects must push past applications and include infrastructure needs for application hosting, networking, and databases.

Information presented in the cloud roadmap company document and all participants discussed the benefits of having a company directive to adopt cloud computing services. IT architects must understand the importance of having senior management's support and endorsement regarding the initiative to reduce TCO within the company. Participant 1 indicated that when attempting to bring business units on board to accepting the company directive, IT architects needed to "explain why the change was needed and if the switch to cloud computing services was worth the effort". Participant 3 indicated that leaders within some business units stated their applications are working just fine on-premise, so why should they move them to the cloud. From an IT perspective, IT architects should always look for ways to become more efficient and evolve. Additionally, IT architects should obtain acceptance from key business units and explaining how adopting cloud comping services will add value to their business processes. Participants 1, 2, 4, and 5 discussed using a cost benefit analysis process for their business unit when adopting cloud computing services. Participant 7 indicated that IT architects should look beyond the normal cost benefit analysis and explain how cloud

computing services provides greater scalability than their current on-premise solutions. An IT architect can explain the benefits of cloud computing services, but without alignment with the company directive, leaders within business units may choose to ignore the company directive and forego moving their business processes to cloud computing services.

In brief, establishing a clear company directive is important in a decision to adopt cloud computing services. A company directive allows IT architects, key stakeholders, and senior management to align on an effective implementation strategy. Additionally, a company directive can prevent stakeholders in business units from opting out of the company cloud computing strategy. Furthermore, a company directive aligns key stakeholders and senior management with the company objective to move 70% of on-premise applications to the cloud within the next three to five years.

Company directive is an external factor that can have an impact on PEOU or PU in the behavioral intent to adopt cloud computing services. Understanding the company directive and strategy for adopting cloud computing services is considered a positive impact on PU for IT architects and key stakeholders. Information stated by participants and reviewed in company documents supports a company directive as a positive impact on PU. A positive impact on PU leads to a positive behavioral intent to adopt cloud computing services. Ambodo, Suryanto, and Sofyani (2017) used the TAM to explore the impact of PEOU and behavioral intent related to the implementation of a new company policy when the change is mandatory. The researchers concluded that the user (employee) perception of the new company policy had a negative impact on PEOU, yet

had positive impact on PU in the intent to adopt a new cloud computing system. Similar to the previous study, the company directive is considered mandatory and will provide guidance and a clear direction for the company to follow. Providing a clear company directive allows key stakeholders to align their key business initiatives and allows employees to understand the strategic value of adopting cloud computing services leading to PU and a positive behavioral intent to adopt cloud computing services. Unlike the previous study, there was not a negative impact to PEOU in the intent to adopt cloud computing services.

Twelve-Factor application methodology. The Twelve-Factor application methodology was a theme that emerged during data analysis and aligns with the implementation strategy in the literature review. Twelve-Factor application methodology is an evaluation process and an important step in an implementation strategy when IT architects decide to migrate applications to the cloud (Khan, 2017). The use of the Twelve-Factor application methodology enables agility in development by providing the appropriate feature sets for applications and infrastructure moving to cloud computing services.

Participants 1, 2, 4, 5, 6, and 7 mentioned using the Twelve-Factor application methodology for building new web applications in the cloud and as an evaluation process (see Table 1). Five company documents contained information supporting the decision to utilize the Twelve-Factor application methodology as an evaluation process. Participant 1 stated “the Twelve-Factor methodology approach is a best practice designed to enable developers to build applications with portability and resilience when deployed to the

web". Participant 2 indicated the Twelve-Factor application methodology allows IT architects to evaluate code supporting business processes for identification, screening and categorization. A review of the Technology Services Overview document indicated that Twelve-Factor application methodology is a design principle to achieve a solution that is anti-fragile, always available, and predictable stable. In prior research, Khan (2017) utilized Twelve-Factor application methodology to identify and implement key mechanisms required for a container orchestration platform in the adoption of cloud computing services. During the evaluation process, application code is compared to the twelve process steps in Table 2 to help determine which processes are cloud ready. Participant 2 indicated "if an application was built with that concept in mind, you're much more likely to be able to move to the cloud with minimal re-architecture or redesign". If an application is deemed not cloud ready, the information in Table 2 allows an IT architect to determine the issue and next steps for code remediation. Understanding how to effectively evaluate an application for cloud adoption will benefit IT architects, business units, and ultimately the company.

Table 2

Twelve-Factor Application Methodology

Step	Factor	Description
1	Codebase	There should be exactly one codebase for a deployed service with the codebase being used for many deployments.
2	Dependencies	All dependencies should be declared, with no implicit reliance on system tools or libraries.
3	Config	Configuration that varies between deployments should be stored in the environment.
4	Backing services	All backing services are treated as attached resources and attached and detached by the execution environment.
5	Build, release, run	The delivery pipeline should strictly consist of build, release, run.
6	Processes	Applications should be deployed as one or more stateless processes with persisted data stored on a backing service.
7	Port binding	Self-contained services should make themselves available to other services by specified ports.
8	Concurrency	Concurrency is advocated by scaling individual processes.
9	Disposability	Fast startup and shutdown are advocated for a more robust and resilient system.
10	Dev/Prod parity	All environments should be as similar as possible.
11	Logs	Applications should produce logs as event streams and leave the execution environment to aggregate.
12	Admin Processes	Any needed admin tasks should be kept in source control and packaged with the application.

In summation, Twelve-Factor application methodology is an evaluation process and an important step in an implementation strategy to adopt cloud computing services. The benefit of using Twelve-Factor application methodology include using declarative formats for setup automation to minimize time and cost as new developers are onboarded to a project. The methodology also allows for a clean contract with the underlying

operating system to offer maximum portability between execution environments. Twelve-Factor applications are designed for deployment on modern cloud platforms and thus eliminating the need for servers and systems administration. Another benefit of Twelve-Factor is the minimalization of divergence between development and production environment which enables continuous integration and continuous deployment. Twelve-Factor applications are designed to leverage the scalability and flexibility of the cloud by scaling up and down without significant changes to architecture or development practices. Finally, Twelve-Factor methodology is code agnostic and will work with applications written in any programming language utilizing any combination of backend services.

Twelve-Factor application methodology is an external factor that can have an impact on PEOU or PU in the behavioral intent to adopt cloud computing services. Utilizing the Twelve-Factor application methodology allows IT architects to determine which applications are cloud ready is considered a positive impact on PEOU and PU. Information stated by participants and reviewed in company documents supports a Twelve-Factor application methodology as a positive impact on PEOU and PU. A positive impact on PEOU and PU leads to a positive behavior intent to adopt cloud computing services. In other research, Amadu, Muhammad, Mohammed, Owusu, and Lukman (2018) used TAM and a check list to determine if social media adoption would be embraced by university students. The researched indicated the acceptance of new technology was based on PEOU (utilizing the checklist) and PU had a positive relationship with collaborative learning via new technology. Schoonenboom (2014)

utilized TAM to assess if using a specific tool, a specific instruction task, and a specific user interface would impact the PEOU or PU in the intent to use a new learning management system. Also, Schoonenboom's research utilized a task level approach similar to the Twelve-Factor application methodology. Schoonenboom's research concluded that using a specific tool, instructions task, and user interface had a positive impact on PEOU and PU in the behavior intent to adopt a new learning management system. Similar to both studies, utilizing a checklist or in this case Twelve-Factor application methodology has a positive impact on PEOU and PU leading to significant behavioral intent to adopt cloud computing services.

Six "R" approach. The Six "R" approach was another theme that emerged during data analysis and aligns with the implementation strategy in the literature review. Six "R" approach is another evaluation process and implementation strategy utilized by IT architects when deciding to adopt cloud computing services (Linthicum, 2017). IT architects must utilize an evaluation process to determine the best adoption plan for cloud computing utilization to support their respective business unit.

Six "R" approach was a theme that six participants discussed and noted was important. Participants 1, 2, 4, 5, 6, and 7 discussed using the Six "R" concept of rehost, replatform, repurchase, refactor, retire, and retain for on-premise solutions moving to the cloud. Additionally, five company documents contained information pertaining to the Six "R" approach (see Table 1). The Technology Services document indicated that the Six "R" approach was a holistic approach to understanding what applications and services key stakeholders within the company want to move and how a migration will affect

licensing, services, and productivity across the organization. The rehost or lift and shift approach allows IT architects to migrate applications to cloud computing services without any code modifications. The rehost approach is faster and less resource intensive but benefits such as elasticity and flexibility are not achieved. Rehost solutions are typically cheaper than on-premise solutions, but are more expensive than replatformed or refactored solutions. The replatform approach allows IT architects to move solutions to the cloud with a small amount of changes. The replatform approach is a compromise between rehost and refactor which offers cloud functionality with optimized cost.

The repurchase approach is moving to a different product and is commonly done when an application is moved to a SaaS solution provider such as Salesforce.com, Workday, etc. A move to a repurchase or SaaS solution is not as simple as some IT architects think. Depending on the solution, IT architects may need to integrate on-premise backend systems with the new repurchase solution which could introduce integration issues. The refactor approach requires an IT architect to rearchitect or recode some portion of an existing solution to take advantage of cloud-native frameworks and functionality. The refactor approach is resource intensive, but allows a solution to take full advantage of cloud-native features to maximize cost and operational efficiency.

The retire approach is simple in concept, but seems to be the hardest option for some insurance companies. Due to the Department of Insurance regulations, some insurance companies are required to maintain legacy systems until all policies are no longer managed on a platform. If a company is not bound by compliance laws, shutting down unused applications may reduce support by a noticeable difference. Retain is the

final approach and usually means do nothing for now, but revisit when opportunity allows.

In conclusion, the Six “R” approach is another evaluation process utilized in an implementation strategy to adopt cloud computing services. The approach focuses on the six concepts of rehost, replatform, repurchase, refactor, retire, and retain for evaluating on-premise solutions moving to the cloud. Furthermore, Six “R” is considered a holistic approach to understanding what applications and services key stakeholders within a company want to move and how a migration will affect licensing, services, and productivity across an organization.

Six “R” approach is an external factor that can have an impact on PEOU or PU in the behavioral intent to adopt cloud computing services. Information stated by participants and reviewed in company documents supports a Six “R” approach as a positive impact on PEOU or PU. The Six “R” approach provides IT architects with an easy method to categorize applications for transitioning to cloud computing services. Additionally, IT architects can use the categorized list to create a roadmap for discussions with key stakeholders. Creating a categorized list in the Six “R” approach can enhance an IT architect’s job which leads to a positive impact on PU and significant impact in behavioral intent to adopt cloud computing services. Hsu and Wu (2017) used TAM to determine if PEOU and PU impacted behavioral intent to use a repurchased cloud nursing information system versus a previous on-premise system. The study indicated that users did not feel the new nursing system was easy to use and many preferred the old system. If a user does not consider a system easy to use, they are unlikely to consider the system

useful. Unlike the previous study, using the Six “R” approach is considered an easy process and a positive impact on PU in the behavioral intent to adopt cloud computing services.

Theme 2: Strategies to Adopt Cloud Services Models

Strategies to adopt cloud services models was another theme that emerged from the interviews and supporting documents. The strategies consisted of buy versus build/SaaS, controlled adoption/PaaS, and lift and shift/IaaS which aligns with the portability strategy in the literature review (see Table 4). Developing an understanding of the different cloud service models is important for any IT architect. Without understanding the advantages and disadvantages, IT architects are not able to recommend valid service offerings to their respective business units. Creating strategies to adopt cloud services models is critical because effective strategies prevents project failures and migration issues which may impact a company’s ability to successfully adopt cloud computing services.

Buy versus build/SaaS. Buy versus build/software as a service (SaaS) was a theme that emerged during data analysis and aligns with the portability strategy in the literature review. Buy versus build/SaaS aligns with the portability strategy because most buy versus build/SaaS solutions entail company data which is easier to move from one vendor to another without portability concerns. A buy versus build/SaaS strategy is also in alignment with the Six “R” approach from Theme 1. Buy versus build/SaaS strategy is utilized when IT architects within a company are no longer interested in hosting or supporting an on-premise solution. Therefore, IT architects must understand the

advantages and disadvantages of moving to a buy versus build/SaaS strategy. Buy versus build/SaaS was a theme discussed by participants in the study. During the analysis phase, I reviewed 11 company documents to understand the benefits of using different cloud service models (see Table 3).

Table 3

Factors for Strategies to Adopt Cloud Services Models

Advantage	Buy versus build SaaS	Controlled adoption PaaS	Lift and shift IaaS
Centrally managed	✓	✓	✓
Remotely hosted server	✓	✓	✓
Accessed via internet	✓	✓	✓
No hardware or software updates by user	✓		
Cost-effective method for application deployment		✓	
Scalable and flexibility	✓	✓	✓
High availability	✓	✓	✓
Customization without maintaining the software		✓	
Reduces coding	✓	✓	
Easy migration to the hybrid model		✓	✓
Most flexible model			✓
Automated deployment of infrastructure		✓	✓
Hardware purchased based on consumption		✓	✓
Clients have full autonomy of infrastructure			✓
Resources purchased as-needed		✓	✓

Table 4

Themes for Strategies to Adopt Cloud Services Models

	Participant		Document	
Theme	Count	References	Count	References
Buy versus build/SaaS	7	35	11	23
Controlled adoption/PaaS	6	25	5	13
Lift and shift/IaaS	6	31	11	23

Participants 1, 2, 3, 4, 5, 6, and 7 indicated the most effective cloud adoption strategy is buy versus build/SaaS which also aligns with the new company directive. Company documents referenced the buy versus build strategy as SaaS based applications or solutions. The Aite Report - Top 10 Trends in Insurance document indicated that healthcare, life, and P&C industries are betting big on digitalization in the form of SaaS, cloud, and online and mobile channels. SaaS is the cloud computing model where customers use a service provider's application running on cloud infrastructure (Loukis, Janssen, & Mintchev, 2019). The underlying cloud infrastructure is not managed by the application provider or the customer, but is managed by the cloud service provider. Additionally, a buy versus build/SaaS strategy enables IT architects to leverage scalability and flexibility of a vended solution without the overhead of maintaining an on-premise solution.

Buy versus build/SaaS was indicated by seven participants which aligned with the company directive and the Twelve-Factor application methodology indicated in the first theme (see Table 1). The buy versus build/SaaS strategy is effective because a buy versus

build/SaaS solution is easier to set up, maintain, and implement than other strategies such as controlled adoption/PaaS or lift and shift/IaaS. Participant 6 indicated using SaaS gives an IT architect flexibility and "if an IT architect does not like a vendor or what a vendor offers, they can easily switch to something different". However, moving from one buy versus build/SaaS provider to another is not as easy as Participant 6 indicated. To move from one provider to another may require breaking a contract, utilizing an opt out clause, or not renewing a contract.

Pay as you go flexibility, scalability, automatic updates, and accessibility were other benefits stated by six of the seven participants. Rather than spending budgets on software installs and additional hardware, IT architects can subscribe to a SaaS offering using pay as you go pricing. The pay as you go pricing model allows IT architects to transition operating costs to a recurring cost which creates a predictable budget for their business units. Participant 6 stated buy versus build/SaaS solutions have scalability in on-demand features and not just services or computing power. Most buy versus build/SaaS solutions are not volume based which allows IT architects to push as much work through the solutions as possible. Two SaaS contracts reviewed during my investigation indicated IT architects utilize volume based and per user solutions. Volume based or per user solutions are usually based on business need. Participant 7 stated a key feature of using a buy versus build/SaaS solution was automatic updates. IT architects can rely on SaaS providers to perform updates and patching which eliminates the need for in-house staff to perform the same functions. SaaS providers must keep their solutions updated and patched because the solution usually provides services to multiple companies. Not

patching a solution can jeopardize solution providers credibility within the industry. Additionally, patching requirements can be written into the service contract. Participants indicated buy versus build/SaaS as a good strategic solution because SaaS applications are delivered over the internet and available to any device with internet access. Enabling a solution over the internet is good for usability, but the approach has challenges such as data exposure.

In essence, buy versus build/SaaS is popular because some IT architects within companies are no longer interested in hosting or supporting on-premise solutions. Additionally, buy versus build/SaaS aligns with a portability strategy because most buy versus build/SaaS solutions entail company data which is easier to move from one vendor to another. In buy versus build/SaaS, the underlying cloud infrastructure is not managed by the application provider or the customer, but is managed by the cloud service provider. Furthermore, a buy versus build/SaaS enables IT architects to leverage scalability and flexibility of a vended solution without the overhead of maintaining an on-premise solution. Finally, pay as you go flexibility, scalability, automatic updates, and accessibility are other benefits of buy versus build/SaaS.

Buy versus build/SaaS is an external factor that can have an impact on PEOU or PU in the behavioral intent to adopt cloud computing services. Information stated by participants and reviewed in company documents supports buy versus build/SaaS as a positive impact on PEOU and PU. Buy versus build/SaaS allows an IT architect to pay for software subscriptions versus developing onsite applications leading to a positive impact on PEOU and PU. If an IT architect is not happy with a SaaS service, they can use

an opt out clause or move to a new provider at contract renewal. Additionally, buy versus build/SaaS is categorized as a positive impact on PEOU and PU because shifting away from application hosting and on-premise hardware will remove certain job responsibilities and enhances job performance. A positive enhancement in job performance has a positive impact on behavioral intent to adopt cloud computing services. Yang and Wang (2019) used TAM to analyze how a user's perceived ease of using a new translation software helped shape a user's perspective concerning PU. The ability of a user to easily utilize the new technology has an impact on the perceived effectiveness of the software. Additionally, Razmak and Bélanger (2018) utilized TAM to analyze patient responses to using a SaaS based personal healthcare system. In the study, healthcare patients found the SaaS solution easy to use and therefore useful. Similar to both of the previous studies, buy versus build/SaaS has a positive impact on PEOU and PU in the behavioral intent to adopt cloud computing services.

Controlled adoption/PaaS. Controlled adoption/platform as a service (PaaS) was a theme that emerged during data analysis and aligns with the portability strategy in the literature review. Controlled adoption/PaaS aligns with the portability strategy because most controlled adoption/PaaS solutions consist of integration points and recoding of applications causing portability issues if not implemented correctly. A controlled adoption concept is also in alignment with the Six "R" approach from Theme 1. The controlled adoption/PaaS is considered a refactor approach of moving on-premise applications to the cloud. The refactor approach requires an IT architect to rearchitect or recode some portion of an existing solution to take advantage of cloud-native frameworks

and functionality (Abdullah, Iqbal, & Erradi, 2019). Therefore, IT architects must understand the advantage and disadvantage of moving on-premise application to a controlled adoption/PaaS strategy.

Participants 1, 2, 3, 4, 6, and 7 indicated that controlled adoption/PaaS was an effective strategy and aligned with the new company directive. Additionally, five company documents reference controlled adoption as PaaS. The company document Cloud Computing Roadmap, discussed controlled adoption/PaaS as a reference architecture to avoid duplicated solutions and drive seamless integration. In a PaaS service model, the customer is responsible for maintaining the application and data (van Eyk et al., 2018). However, the cloud service provider is accountable for the runtime environment, middleware, operating system, servers, storage, and networking. The use of a controlled adoption/PaaS service model provides IT architects with the ability to leverage scalability and flexibility for application development environments. Additionally, PaaS providers offer solution packages with specific characteristics that provide all phases of the system development lifecycle using APIs or gateway software.

Participants 1, 2, 3, 4, 6, and 7 indicated using APIs and gateway software allows for easy creation of application environments but exposed the company to portability issues. Participant 7 stated most companies new to adopting cloud computing services fall into the mistake of using native APIs and refactoring their code which leads to portability issues. The best way for a company to avoid compatibility or portability issues while using APIs is to leverage an infrastructure as code framework. Leveraging an infrastructure as code framework allows IT architects to define data center infrastructure

in a high-level configuration language. The high-level language is used to create an execution plan to build infrastructure in service providers such Amazon Web Services, Microsoft Azure, IBM, and Google Cloud Platform ("Method of cloud", 2018). Additionally, using an infrastructure as code framework allows IT architects within a company to deploy the same PaaS environments regardless of cloud service provider making portability a nonissue.

Participants 1 and 7 discussed using application containers along with pivotal cloud foundry to ensure DevOps teams can deploy applications consistently throughout the software release process. Application container images are usually created using a structured layer of common based functionality that may be reused by multiple container images. Using the layered approach on top of a base image enables DevOps team to only update the modified layers when transferring images between deployment environments. Additionally, the participants indicated the approach can reduce deployment time, improve testing, and allow the creation of a continuous improvement/continuous deployment pipeline. However, the participants indicated each container image must contain every runtime dependency of the packaged application. The runtime dependency leads to more images and larger numbers of active containers which ultimately lead to fragmentation of deployed runtime dependencies causing issues in the adherence policy for security, compliance and regulatory requirements. Participant 7 discussed the need for a governance mechanism to onboard and offboard development environments. The governance mechanism guarantees that development environments are time boxed and

removed after a certain number of days. The removal of unused development environments will help manage cost for controlled adoption/PaaS.

As indicated above, the controlled adoption/PaaS is considered a refactor approach of moving on-premise applications to the cloud. Controlled adoption/PaaS aligns with the portability strategy because most controlled adoption/PaaS solutions consist of integration points and recoding of applications causing portability issues if not implemented correctly. The controlled adoption/PaaS approach requires an IT architect to rearchitect or recode some portion of an existing solution to take advantage of cloud-native frameworks and functionality. However, refactoring controlled adoption/PaaS solutions using native APIs can lead to portability issues. To alleviate portability issues with controlled adoption/PaaS, IT architects can leverage an infrastructure as code framework. Using an infrastructure as code framework allows IT architects to define data center infrastructure in a high-level configuration language within various cloud service providers.

Controlled adoption/PaaS is an external factor that can have an impact on PEOU or PU in the behavioral intent to adopt cloud computing services. Information stated by participants and reviewed in company documents supports a controlled adoption/PaaS as an impact on PEOU and PU. The positive impact on PU is because a controlled adoption/PaaS allows an IT architect to enable PaaS development environments and continuous integration/continuous deployment with infrastructure as code or application containers. However, controlled adoption/PaaS could have a negative impact on PEOU depending on the method of deployment chosen by the IT architect. If an IT architect

chooses to utilize controlled adoption/PaaS using native cloud vendor APIs, there could be complications leading to a negative impact. Additionally, a negative impact in PEOU can negatively impact PU and the behavioral intent to adopt cloud computing services. Esteban-Millat, Martínez-López, Pujol-Jover, Gázquez-Abad, and Alegret (2018) used TAM to analyze how a user's perceived ease of using a virtual learning environment impacted a user's PU and willingness to use virtual learning environments. The study concluded that users perceived the new learning environment was easy to use and useful indicating a positive impact on PEOU and PU in the behavioral intent to use the new virtual learning environments. Unlike the previous study, controlled adoption/PaaS does not have a clear positive or negative impact on PEOU or PU in the behavioral intent to adopt cloud computing services. The positive or negative impact on PEOU or PU is driven by the difficulty of the refactored application and the decision to use native APIs versus infrastructure as code or containers.

Lift and shift/IaaS. Lift and shift/infrastructure as a service (IaaS) was a theme that emerged during data analysis and aligns with the portability strategy in the literature review. Lift and shift/IaaS aligns with the portability strategy because most lift and shift/IaaS solutions consist of integration points which can cause portability issues if not implemented correctly. Lift and shift/IaaS is also in alignment with the Six "R" approach from Theme 1. Lift and shift/IaaS is considered the rehost approach of moving on-premise applications to the cloud. The rehost approach allows application migrations to cloud computing services without code modifications. The strategy is faster and less resource intensive, but benefits such as elasticity and flexibility may not be achieved.

Therefore, IT architects must understand the advantages and disadvantages of moving on-premise hardware to the cloud using a lift and shift/IaaS strategy.

Participants 1, 2, 4, 5, 6, and 7 indicated the least effective cloud adoption strategy was lift and shift/IaaS (see Table 4). Additionally, 11 company documents were reviewed and referenced lift and shift/IaaS. The Technology Blue Paper listed on the company intranet indicated that IaaS has opportunity for insurers to lower their IT hardware run costs by taking advantage of cloud computing infrastructure where possible (some legacy applications will likely have to be run on specific hardware). IaaS is the cloud computing model with infrastructure such as storage, servers, and central processing through the use of virtual machines (Adhikari, Nandy, & Amgoth, 2019). IaaS is considered the fastest growing cloud services model because a cloud service provider can combine virtual machines and data storage into one platform with minimal resource management.

According to Linthicum (2017), a lift and shift/IaaS strategy or rehost approach allows application migrations to cloud computing services without code modifications. Participants 3 and 4 indicated the key adoption point of cloud computing is the ability to scale up additional severs during peak processing and scale down when not in use which should provide more processing power at a lower cost. Scalability and flexibility are selling points for cloud computing services the appropriate steps must be taken. IT architects must decide if they want to use on-demand servers or a pool of servers for peak processing. Using on-demand servers cost more than using a pool due to the cloud server

provider spinning up virtual servers at will. Understanding the difference in functionality and business need is critical for IT architects using a lift and shift/IaaS strategy.

Lift and shift/IaaS solutions are typically cheaper compared to on-premise solutions, but are more expensive than replatformed or refactored solutions as mentioned in Theme 1. Participants 1, 2, and 7 indicated lift and sift solutions appear cheaper, but eventually the cost savings are neglectable because most IT architects within a company do not take time to plan an effective lift and shift/IaaS strategy. Some IT architects implement a lift and shift/IaaS strategy using a one to one hardware ratio. In essence, the IT architects are attempting to recreate their on-premise infrastructure in the cloud. Recreating an on-premise environment negates the scalability and flexibility benefit of using cloud computing services.

Participant 7 indicated IT architects within companies need complete visibility into all enterprise infrastructure to accurately determine which workloads should move to the cloud or stay on-premise. If an IT architect has complete visibility into the enterprise infrastructure, the IT architect can design and implement cloud solutions utilizing the scalability and flexibility of the cloud. To effectively implement a cloud solution, IT architects need to understand peak processing time and understand end to end service level agreements between business entities. Participant 7 stated analysis is required to understand total cost of ownership (TCO). To perform a true TCO analysis, IT architects should have an understanding of cloud cost complexities, understand company workload needs, and how to use an effective cloud cost analysis tool. A cloud analysis tool is recommended because cloud pricing can vary by provider. A virtual server deployed on

AWS has a different cost than a server deployed on Microsoft Azure. Participants 1 and 2 indicated some users within a business unit thought the number one driver for moving applications to the cloud was to reduce TCO. Moving to cloud computing services is not always about money. Some cloud solutions are actually more expensive than on-premise solutions. IT architects should understand the cost factor when implementing a cloud strategy.

Participant 4 indicated IT architects "preferred to stay away from lift and shift and IaaS if possible, but IT architects understand an IaaS strategy has a purpose". Lift and shift/IaaS allows an IT architect to migrate a solution then perform analysis to improve the solution during multiple iterations. Participant 3 indicated some IT architects were open to using a lift and shift strategy provided the use case was for storage or database usage. Some companies are starting to augment on-premise systems using cloud computing services for peak processing needs. When companies need additional processing for data analytics etc., many of the companies utilize compute power from AWS, Microsoft Azure, or Google. Companies that utilize this model, pay for extra compute power when needed unlike paying for an on-premise server regardless of usage.

Given the above information, lift and shift/IaaS is important in a decision to adopt cloud computing services. Lift and shift/IaaS aligns with the portability strategy because most lift and shift/IaaS solutions consist of integration points which can cause portability issues if not implemented correctly. Lift and shift/IaaS is considered the rehost approach of moving on-premise applications to the cloud. The rehost approach allows IT architects to migrate applications to cloud computing services without code modifications. Some IT

architects implement a lift and shift/IaaS strategy using a one to one hardware ratio from on-premise to cloud leading to an ineffective cost management. Lift and shift/IaaS solutions are typically cheaper compared to on-premise solutions, but are more expensive than replatformed or refactored solutions. However, the strategy is faster and less resource intensive, but benefits such as elasticity and flexibility may not be achieved.

Lift and shift/IaaS is an external factor that can have an impact on PEOU or PU in the behavioral intent to adopt cloud computing services. Information stated by participants and reviewed in company documents supports lift and shift/IaaS as an impact on PEOU. Utilizing lift and shift/IaaS allows an IT architect to quickly move on-premise solutions to a cloud service provider without a lot of planning. Moving solutions without a lot of planning is viewed as free of effort and a positive impact on PEOU. Verma, Bhattacharyya, and Kumar (2018), TAM was used to determine if perceived usefulness had a positive influence on attitude and behavioral intention to adopt a big data analytics system. The study concluded that PEOU had a positive impact on PU and the intent to use the big data analytics system. Similar to the recent study, the use of lift and shift/IaaS in this study has a positive impact on PEOU and PU in the behavioral intent to adopt cloud computing services.

Theme 3: Strategies to Adopt Cloud Computing Models

Additional information was obtained from reviewing the interview transcripts and company documents to compare the benefits and limitations of using different cloud computing models (see Table 5). The additional analysis of the information allowed me to ascertain effective strategies used by IT architects when adopting cloud computing

models. The effective strategies defined by the participants and company documents were public cloud, hybrid cloud, and private cloud (see Table 6). Each participant indicated they were aware of and following the new company directive to move as many business applications to the cloud using secure, efficient, and cost-effective strategies. The overall goal of the company is to move 70% or more of the current applications to the cloud within the next few years. Additionally, each participant explained that IT architects within the company would have a hard time achieving such a feat because many applications within the company are running on legacy platforms. Because of legacy applications and high mainframe usage, participants indicated the strategy within the company is to use a combination of cloud computing models such as public cloud, hybrid cloud, and private cloud.

Public cloud. Public cloud was a theme that emerged during data analysis and aligns with the compatibility strategy in the literature review. Public cloud aligns with the compatibility strategy because most public cloud solutions require integration which can cause compatibility issues if not properly configured. A public cloud offering is an option for a company wanting scalability and flexibility in hardware, utility style pricing, and do not wish to invest or maintain on-premise infrastructure (see Table 6). IT architects must understand the advantages and disadvantages of implementing a public cloud strategy.

Public cloud was a theme discussed by Participants 1, 2, 3, 4, 5, 6, and 7 in the study. A public cloud is a cloud offering maintained for generic public use by a third-party entity based on a pay as you go pricing structure (Han, Li, & Chen, 2019). Based on information obtain from the Cloud Computing Roadmap document and interviews from

IT architects, the company plans to utilize public cloud as the main cloud computing model. From a leadership directive and application roadmap point of view, the move to public cloud is consistent with previous research found in the literature review. Participant 7 indicated getting out of the infrastructure business is the overall goal for the company. The no infrastructure goal or new directive may allow IT architects within the company to focus on new and innovative products and applications. The focus on innovative products and application instead of infrastructure may differentiate the company from competitors within the insurance industry.

Table 5

Factors for Strategies to Adopt Cloud Computing Models

	Public Cloud	Hybrid Cloud	Private Cloud
Advantage			
No investments and maintenance of IT infrastructure	✓		
High scalability and flexibility for unpredictable processing	✓		
Reduction of on-premise IT expertise due to vendor management of infrastructure.	✓		
Utilities style pricing model SLAs and compute needs	✓	✓	
Cost flexibility allows for lean growth strategies for companies	✓		
Flexible policy-driven deployment to allow workload distribution across public and private infrastructure environments		✓	
Scalability of on-premise IT workloads without exposing sensitive information		✓	
High availability and reliability due to multiple data centers and an on-premise infrastructure		✓	
Dedicated secure environment for one organization			✓
High SLA performance and scalability			✓
Scalability and efficiency without compromising security and performance			✓
Compliance to specific regulations			✓
Limitations			

Overall expenses can increase for midsize to large enterprises	✓		
Exposure of sensitive mission information and critical IT workloads	✓		
Regulatory compliance due to low/no visibility and control of infrastructure	✓		
May become expensive if not planned accordingly		✓	
Extensive compatibility and integration issues due to lack of direct control over infrastructure		✓	
Overall complexity for company IT staff to maintain hybrid solution		✓	
Expensive to maintain			✓
Limited access for mobile users			✓
Infrastructure may not offer scalability and flexibility			✓

Table 6

Themes for Strategies to Adopt Cloud Computing Models

	Participant		Document	
Theme	Count	References	Count	References
Public Cloud	7	39	43	78
Hybrid Cloud	5	17	31	35
Private Cloud	2	17	13	23

The benefits of public cloud may entice IT architects within companies to move their applications but public clouds are not without faults. IT architects moving to public clouds must make sure company data is secure. Data security is a major concern for public cloud users. As a part of a data strategy, IT architects must reassure key stakeholders that company data is not being accessed or used illegally by anyone including the cloud service provider.

Participants 1, 2, 5, and 7 discussed limitations such as cost for multinational enterprises (MNEs), exposure of sensitive crown jewel information, and regulatory compliance issues due to low visibility or control of cloud infrastructure (see Table 5). To address cost concerns, IT architects can utilize a cloud cost analysis tool and focus more attention contracts related to cloud computing services. Additionally, IT architects should perform a total cost of ownership (TCO) analysis. To perform a TCO analysis, IT architects should have an understanding of cloud cost complexities, understand company workload needs, and how to use an effective cloud cost analysis tool. Utilization of a cloud analysis tool is recommended because cloud pricing vary by provider. However, the issue of exposing sensitive crown jewel information is mitigated by not putting important data in the public cloud. If an IT architect does not have the option to keep sensitive company data on-premise, encryption is required for data in transit and at rest. Some public cloud vendors are not willing to expose audit logs because public clouds are shared environments and exposing audit logs could expose the vendor to other vulnerabilities. As a mitigation plan, IT architects can ask public cloud vendors to provide audit logs on a specific schedule containing company specific information per contract terms.

Participant 7 stated to successfully migrate to a public cloud will require a thorough implementation strategy. A thorough implementation strategy is required because most public cloud solutions require some type of integration with on-premise systems. Unless the solution is a pure SaaS solution, integration and security measures

are required. Integration and security measures depend on the solution being implemented by the company and the cloud services provider.

In essence, a public cloud is an important model in the decision to adopt cloud computing services. Also, public cloud aligns with the compatibility strategy because most public cloud solutions require integration which can cause compatibility issues if not properly configured. A public cloud offering is an option for most companies wanting scalability and flexibility in hardware and utility style pricing without maintaining on-premise infrastructure. However, the benefit of moving application to a public cloud is not without faults. IT architects moving to public clouds must make sure company data is secure because data security is a major concern for public cloud users. IT architects must reassure key stakeholders that company data is not being exposed to unauthorized entities. Finally, IT architects should perform a TCO analysis to gain an understanding of cloud cost complexities based on company workload needs.

Public cloud is an external factor that can have an impact on PEOU or PU in the behavioral intent to adopt cloud computing services. Information stated by participants and reviewed in company documents supports public cloud as a positive impact on PU and undefined for PEOU. Utilizing a public cloud model in the decision to adopt cloud computing services is considered a positive impact on PU because IT architects are no longer maintaining applications and hardware on-premise. However, the PEOU construct is either positive or negative depending on the solution moving to a public cloud. Integration, security issues, and compliance can cause PEOU to have a negative impact on an IT architect’s behavioral intent to adopt cloud computing services. Akman and

Mishra (2015) were able to determine the PEOU and PU constructs applied to users adopting green information communication technology in public clouds. The researchers concluded that PEOU and PU were positive, but were based on other external factors such as cultural, social, geographical, and economic factors. Similar to Akman and Mishra's study, there is an impact on PEOU and PU, but PEOU is determined based on other external factors such as integration, security, and compliance. The additional external factors are based on the application chosen for cloud migration to a public cloud.

Hybrid Cloud. Hybrid cloud was a theme that emerged during data analysis and aligns with the compatibility strategy in the literature review. Hybrid cloud aligns with the compatibility strategy because most hybrid cloud solutions require complex integration which can cause compatibility issues if not properly implemented. A hybrid cloud allows critical applications or systems containing sensitive data running on infrastructure in a private data center to extended to an external cloud. IT architects must understand the advantages and disadvantages of implementing a hybrid cloud strategy.

During the analysis phase, Participants 2, 3, 4, 5, and 7 discussed hybrid computing as a viable option for adopting cloud computing services for the company. Additionally, 13 documents reviewed contained a reference to hybrid cloud as a company option. According to the Technology Organization company document, insurance companies should take a hybrid approach, incorporating the advantages of both private and public clouds in order to ensure information security and regulatory compliance.

The participants discussed advantages including pay as you go pricing, flexible workload distribution, availability and reliability (see Table 5). Participants listed

limitations including cost creep, compatibility, integration issues, and complexity for on-premise IT staff (see Table 5). A hybrid cloud solution can allow IT architects within a company to move less critical applications or systems to a public cloud to extend compute power cheaper than adding on-premise servers and storage. Participants 2, 3, 4, 5, and 7 discussed using a hybrid cloud solution as IaaS when additional processing power or storage is needed. The company can augment on-premise systems using cloud computing services for peak processing needs similar to large reports or storing large amounts of data for archival purposes.

Participant 2 indicated data scientists within the company attempted to build multiple Hadoop environments, but most of the environments went unused between spikes and were not considered cost effective. Instead of paying for multiple on-premise Hadoop environments, IT architects can save money via TCO and use AWS, Microsoft Azure, or Google for data analytics. All three cloud service providers offer peak processing solutions via on demand virtual servers or virtual standby servers as needed.

Participant 7 discussed using infrastructure as code, server templates, and application containers to scale additional servers as needed to resolve complex integration issues. Similar to controlled adoption/PaaS strategy in Theme 2, IT architects can leverage infrastructure as code to define on-demand servers within cloud data centers using a high-level configuration language. Participant 7 discussed the complexity of integrating on-premise infrastructure with cloud infrastructure. To help alleviate integration issues, IT architects can use an exchange service. The use of an exchange service allows IT architects to focus on utilizing a hybrid cloud approach without using

native virtual private network connections such as AWS Direct Connect, Azure ExpressRoute, etc. The removal of using native APIs or connections will also remove portability concerns.

To summarize, a hybrid cloud is important in a decision to adopt cloud computing services. Hybrid cloud aligns with the compatibility strategy because most hybrid cloud solutions require complex integration which can cause compatibility issues if not properly implemented. A hybrid cloud allows critical applications or systems containing sensitive data running on infrastructure in a private data center to extended to an external cloud. Additionally, IT architects can save money via TCO by using AWS, Microsoft Azure, and Google for peak processing. A hybrid cloud solution is faster and less expensive than adding on-premise servers and storage that is under utilized during non-peak times.

Hybrid cloud is an external factor that can have an impact on PEOU or PU in the behavioral intent to adopt cloud computing services. Information stated by participants and reviewed in company documents supports hybrid cloud as a positive impact on PU and undefined for PEOU. Integrating a hybrid cloud with on-premise servers to can enhance an IT architects job performance making a positive impact on PU. The PEOU construct is either positive or negative depending on the solution moving to the cloud. Integration, security issues, and compliance can cause PEOU to have a negative impact. However, the use of infrastructure as code, container management, and an exchange service can have a positive impact on PEOU when adopting a hybrid cloud solution. Helia, Asri, Kusrini, and Miranda (2018) conducted research to determine if the PEOU

and PU constructs had a positive impact on a hospital employee's behavioral intention to adopt a new hospital information system. The researchers concluded that users of the system considered the new system easy to learn and operate leading to positive impact on PEOU and PU in the behavioral intent to adopt the new hospital information system. Similar to my research, there was a positive impact on PU. However, the two studies differed concerning PEOU because positive or negative impact to PEOU in this study is based on additional external factors such as cost variance, compatibility, integration issues, and complexity. The additional external factors are based on the application chosen for cloud migration to a hybrid cloud.

Private cloud. Private cloud was a theme that emerged during data analysis and aligns with the compatibility strategy in the literature review. Private clouds are considered a better option for IT architects employed in larger companies. Larger companies with private clouds are better suited to address service outages, security failures, and have enough resources to avoid a breach of service levels (see Table 5). IT architects must understand the advantages and disadvantages of implementing a private cloud strategy.

Private cloud was a theme discussed by two participants and was referenced in 13 company documents (see Table 6). During the analysis phase, two participants discussed private cloud computing. Although two participants discussed private cloud, private cloud is not considered a viable option based on the company directive. A private cloud contains data and processes managed by a company IT department. Private clouds are not limited by network, security, or legal restrictions (Jeganathan, 2019). Participants 3 and 6

discussed advantages of a private cloud. A private cloud is dedicated secure environment for one organization that allows scalability and efficiency without compromising security or performance. Furthermore, a private cloud removes concerns for compliance pertaining to specific regulations. Participants 3 and 6 discussed various private cloud limitations. The limitations included being expensive to maintain, limited access to mobile users, and infrastructure may not offer true scalability and flexibility. Traditionally, private clouds are considered better options for IT architects employed in larger companies. Larger companies tend to enough resources to maintain a private cloud, address service outages, security failures, and production service levels. Although information exist that indicate a private cloud can be a viable option, leadership and IT architects are not planning to invest in private clouds as a strategy.

In short, a private cloud is a dedicated secure environment for one organization that allows scalability and efficiency without compromising security or performance. Private clouds are usually on-premise solutions for larger corporations or an offering provided by another company such as Salesforce or IBM. Unlike public clouds, private clouds are not hindered by specific regulations for data and storage retentions. However private clouds are considered expensive to maintain, have limited access for mobile users, and the om-premise infrastructure may not offer true scalability and flexibility.

Private cloud strategy is an external factor that can have an impact on PEOU or PU in the behavioral intent to adopt cloud computing services. Information stated by participants and reviewed in company documents supports a private cloud as negative impact on PEOU and a positive impact on PU. Creating and maintaining an on-premise

private cloud has a negative impact on PEOU because of maintaining the environment. A private cloud has a positive impact on PU because an IT architect will no longer worry about security and compliance issues found in a public cloud. The company directive to use a public cloud versus private cloud can have a negative impact on PEOU driving negative impact on PU in the behavioral intent to utilize a private cloud. Rahi, Ghani, and Alnaser (2017) conducted research to determine if the PEOU and PU constructs had a positive impact on banking customers behavioral intention to use internet banking. The research indicated there was a negative impact on PEOU because participants indicated the new system was complicated and not easy to use. Similar to my research, the intention to use a new technology was based on PEOU. In TAM, PEOU has the ability to influence PU and the behavioral intent to adopt new technology. In this instance, private cloud had a negative impact on PEOU based on creating an on-premise private cloud and the company directive. The negative PEOU impact is a direct driver to the negative impact of PU. If a private cloud is too difficult to implement and maintain, IT architects will not find value in the use.

Theme 4: Concerns Affecting Strategies to Adopt Cloud Computing Services

Data concerns, security concerns, privacy concerns, and service level agreement emerged as concerns affecting strategies to adopt cloud computing services. A combination of all four concerns emerged as the fourth and final theme (see Table 7). Each participant indicated they were aware of certain concerns affecting the adoption of cloud computing services, but the cost benefit analysis and return on investment was

worth the risk. Additionally, each participant indicated they needed to take certain precautions to address each concern.

Table 7

Themes for Concerns Affecting Strategies to Adopt Cloud Computing Services

	Participant		Document	
Theme	Count	References	Count	References
Data Concerns	7	28	13	38
Security Concerns	6	21	24	51
Privacy Concerns	5	14	10	21
Service Level Agreements	3	11	4	12

Data concerns. Data concerns was a theme that emerged during data analysis and aligns with various sections of the availability, confidentiality, integrity, and privacy strategies in the literature review. Data availability, data integrity, and data ownership in the cloud is considered a major concern for customers planning to adopt cloud computing services. IT Architects must become familiar with techniques to secure data in the cloud.

Data concerns were mentioned by Participants 1, 2, 3, 4, 5, 6, and 7. Also, 13 company documents referenced data concerns related to cloud computing services (see Table 7). Participant 7 indicated that data security is important to any company. The protection of company data is paramount for any company regardless of industry. Each industry may have specific laws concerning data storage and retention, but industry must take steps to protect company data. Participant 3 indicated “once a company’s reputation is impacted, customers may lose trust in the company’s ability to keep their information

safe". The document Business Information Service Office strategy document indicates that the company crown jewel data must have multiple forms of security to increase the required effort for an adversary. To help mitigate data concerns, IT architects can implement a data integrity strategy focused on data signing, whole file checking, encrypting data resting and inflight, and implementing a software integrity check. Additionally, IT architects can utilize secure socket layer (SSL) and transport layer security (TLS) to prevent network sniffing and spoofing attacks. In addition to SSL and TLS, a key management system can prevent a man in the middle exploitation of data between the customer and the cloud service provider.

Participants 3 and 4 discussed data availability being a critical component for adopting cloud computing services. In an effort to overcome the issue with data availability, IT architects can use a combination of on-premise storage and cloud backup provided by the cloud service provider. Another method to help with data availability is using a two data center or zonal approach. Major cloud computing host such as Microsoft Azure and AWS have multiple data centers in a geographical location. IT architects can setup data replication between data centers to provide data redundancy and availability.

Participants 1 and 2 were concerned about who owns data in the cloud and the return policy when a contract ends. Data processed or used for transactions in the cloud is the responsibility of the company using the cloud computing services. The SaaS contract I reviewed has specific verbiage indicating that upon termination of the contract or written notice, the vendor must purge company data from all vendor systems.

Additionally, the contract specifically indicates the customer (company) has 30 days to obtain data from the vendor systems.

Participant 2 discussed needing verbiage in the contract pertaining to recovery time objective and recovery point objective of data for normal day to day activity. The recovery point objective and recovery time objective depends on the cloud service provider's disaster recovery plans and if a customer is willing to pay for replication between data centers. Participant 3 discussed needing verbiage in the contract pertaining to disaster recovery. Mendonça, Andrade, Endo, and Lima (2019) indicated a replication disaster recovery between cloud data centers is sometimes referenced as dual zone and restoring from backup is a single zone. Dual zone replication can provide a recovery time objective less than 1 hour, and a recovery point objective less than 15 minutes. If cloud services customers do not view their data as business critical, a customer may choose to use a simple disaster recovery plan of restoring in a different data center. Restoring from backup in another location can have a recovery time less than 48 hours and a recovery point of less than 1 hour.

In essence, data concerns was a theme that emerged during data analysis and aligns with various sections of the availability, confidentiality, integrity, and privacy strategies in the literature review. The protection of company data is paramount for any company regardless of industry. Each industry may have specific laws concerning data storage and retention, but industry must take steps to protect company data. Cloud computing services contracts should have verbiage indicating what steps the vendor should take to return company data and expected timeline. Additionally, the contract

verbiage should require the cloud service providers to purge all vendor systems of customer data. Finally, IT architects should understand different steps to guarantee data availability and integrity.

Data availability, data integrity, and data ownership concerns are external factor that can have an impact on PEOU or PU in the behavioral intent to adopt cloud computing services. Information stated by participants and reviewed in company documents supports data concerns as a negative impact on PEOU and PU. Implementing certain measures to protect company data and guarantee data availability is not an easy task leading to negative impact on PEOU. If IT architects do not perceive implementing certain measures to protect and guarantee data as stress free, they will opt not to use the measures leading to a negative impact to PU. A negative impact in PEOU and PU leads to negative behavioral intent for a user to adopt cloud computing services. Chen, Xu, and Arpan (2017) conducted research to determine if the PEOU and PU constructs had a positive impact on participants behavioral intention to adopt smart meter technology. The researcher concluded that the new smart meters were easy to use, but participant were still reluctant to use them because of data and privacy concerns. Similar to this research, the intention to use a new technology was based on data concerns impacting PEOU and PU. The new technology is easy to use and has a positive impact on PEOU, but data concerns prevent users from adopting the technology. If a user has data and privacy concerns, they will not think the system is useful driving a negative impact on PU. In this research, data availability, data integrity, and data ownership concerns had a negative impact in PEOU and PU.

Security concerns. Security concerns was a theme that emerged during data analysis and aligns with the security strategy in the literature review. Security in the cloud is considered a major concern for customers and the cloud service provider. Security in the cloud encompass application security, physical/technical equipment, and includes procedures for security guidelines.

Security was a concern mentioned by Participants 1, 2, 3, 4, 5, and 7. Additionally, 24 company documents referenced security related to cloud computing services. Participants 1 and 2 discussed utilizing the Twelve-Factor application methodology and application containers would help with application security. Utilizing the Twelve-Factor methodology requires a developer to think about security as code is written and not as an afterthought. Along with building security into code, IT architects can extend their security policies and access control lists to the cloud by linking on-premise active directory with the cloud service provider active directory. Participants 1 and 7 indicated that security professionals should build application containers and virtual server templates to increase application security. Application containers and virtual server templates enables the security team to build in security measures based on company guidelines. The containers and templates are used to keep other IT architects from creating nonstandard deployments leading to security vulnerabilities. The Cloud Security Framework (CSF) company document states that a security framework is cloud agnostic allowing company best practices to apply to any cloud service provider. The CSF framework enables consistency across cloud providers by using agnostic terms such as Tenant, Zone and Sub-Zone. The goal of the CSF is to gain alignment on specific

security controls that are applied to assets as the assets move to a public cloud hosting provider. Utilizing application containers, virtual server templates and following the CSF, IT architects can help mitigate exposing the company to unacceptable risk.

Participant 7 indicated that intrusion monitoring was another concern with cloud computing. Normal monitoring tools are appropriate for detecting intrusion on physical networks, but are not as effective on virtual networks. To monitor virtual networks, IT architects must deploy virtual security appliances. A virtual security appliance is a network security service running entirely within a virtualized environments and place between multiple network segments ("Virtual security appliances", 2015). A virtual security appliance must be encapsulated and dynamically deployed within a cloud service provider's environment to protect the multiple virtual networks. However; many cloud service providers do not allow customers to perform intrusion tests or place virtual appliances within their environments.

Participant 3 discuss the company directive that all SaaS solutions must provide single sign on (SSO). Single sign on is implemented by extending the on-premise active directory service to a specific cloud vendor. Cusack and Ghazizadeh (2016) indicated there is no model that can provide system integrity verification in the cloud SSO framework. However, IT architects can take precautions to make sure SSO is only allowed through a virtual private network (VPN) connection. If a user is not connecting from a company office network, IT architects can require multi-factor authentication to establish a VPN before invoking SSO to a cloud service provider.

Participants 2 stated IT architects within a company should require specific verbiage in cloud computing contracts to access cloud service provider logs. A request to examine cloud service provider logs allows company security professionals to utilize application and management tools to validate if any intrusions were detected and what action was taken to remediate or mitigate the intrusion. Additionally, access to cloud service provider logs provide information to assist the cloud service provider and cloud customer with gateway monitoring to limit surface attacks, monitoring for specific events, exchange of security tokens, and policy enforcement. The company document Cloud Configuration Management outlines that audit logs for intrusion detection, file integrity monitoring and web application firewalls must go to the security account. Additionally, the document indicates that a tool must be used for log aggregation and correlation.

Participants 1 and 7 indicated the company was concerned about threats via APIs. To help alleviate the threat from APIs, IT architects can leverage an infrastructure as code framework to remove the need of using native cloud APIs. IT architects can also use application containers and an exchange service to remove security concerns of using native APIs or connections. Participant 2 indicated security is a concern but stated “there's been a number of surveys and research done to prove that cloud infrastructure can be as secure if not more secure than what most organizations have in their own data centers”. On-premise solutions are more at risk because on-premise infrastructure is consolidated in one place and security is limited by on staff security personal. IT

architects may have limited security expertise, but a cloud service provider may have the ability to afford the best and brightest in cloud computing security.

Given the above information, security concerns was a theme that emerged during data analysis and aligns with the security strategy in the literature review. Security in the cloud is considered a major concern for customers and the cloud service provider. Security in the cloud encompass application security, physical/technical equipment, and includes procedures for security guidelines. IT architects can utilize Twelve-Factor methodology requiring developers to think about security as code is written. Additionally, application containers and virtual server templates allow security teams to build in security measures based on company guidelines. Finally, an IT architect can request copies of cloud service provider logs to perform gateway monitoring of surface attacks, monitoring for specific events, exchange of security tokens, and policy enforcement.

Security concerns is an external factor that can have an impact on PEOU or PU in the behavioral intent to adopt cloud computing services. Information stated by participants and reviewed in company documents supports a security concern as a negative impact on PEOU and PU. Implementing security measures to protect company assets is not an easy task leading to negative impact on PEOU. If IT architects do not perceive implementing security measures as stress free, they will opt not to use the measures leading to a negative impact to PU. A negative impact in PEOU and PU leads to negative behavioral intent for a user to adopt cloud computing services. Taherdoost (2018) conducted research to determine if the PEOU and PU constructs had a positive

impact on participants behavioral intention to adopt e-service technology. In his research, Taherdoost was able to determine that security was an external factor negatively impacting PEOU and PU in the behavioral intent to adopt a new e-service technology. In both studies, security had a negative impact on PEOU and PU in the behavioral intention to use a new technology.

Privacy concern. Privacy concern was a theme that emerged during data analysis and aligns with the privacy strategy in the literature review. Privacy concern is deemed so important that IT architects for various business units perceive privacy as the major concern for stakeholders and customers. Due regulatory compliance, IT architects must account for privacy laws in their strategy to adopt cloud computing services.

Privacy was a concern mentioned by Participants 2, 3, 4, 6, and 7. Also, 10 company documents referenced privacy concerns related to cloud computing services (see Table 7). Participants indicated that customer privacy was a major concern for their business unit and ultimately the customer. IT architects can address privacy concerns by understanding privacy laws, limiting secondary usage of company data via structured contracts, and understanding trans-border data laws pertaining to data being shared by a cloud service provider and a subcontractor.

Participants 2, 3, 4, 6, and 7 indicated that not protecting customer privacy can lead to lack of trust in the company and loss of market share. Participant 2 stated “cloud computing services as a whole is a new area and we don't really know it well enough to feel comfortable putting our crown jewels or critical information out there to potentially be seen by somebody else”. IT architects can help mitigate privacy concerns by requiring

cloud service providers to follow regulatory guidelines for Health Insurance Portability and Accountability Act (HIPAA), Personal Identifiable Information (PII), Personal Card Industry Data Security Standards (PCI-DSS), Sarbanes-Oxley Act (SOX), and the Department of Insurance (DOI) for each state containing policy holders.

Participants 2 and 7 indicated a customer privacy policy must extend beyond on-premise confines to the cloud service provider. The Information Security and Assessment company document indicates all cloud services suppliers are required to agree, in writing, to abide by Supplier's privacy and security program(s), policies, procedures, standards, and processes. Participants 2, 3, 4, and 6 indicated that contracts should stipulate data must not leave the continental United States nor shared with subsidiaries/additional business units of the cloud service provider. In previous research, Gashami et al. (2016) research explained the limitations of trans-border data laws pertaining to data being shared by a cloud service provider and a subcontractor.

Participants 2, 3, 4, 6, and 7 discussed the method of least privilege access. IT architects can establish least privilege access by extending the on-premise active directory and syncing with the version provided by the cloud service provider. Some IT architects may choose to use a directory as a service option to manage both cloud and on-premise assets. Participant 7 discuss adding contract verbiage to limit cloud provider access. The contract should clearly state that non-essential cloud service provider employees should not have access to customer data. For example, an employee may have access to restore data to a certain recovery point, but is not required to have access to read the recovered data.

In brief, privacy concern was a theme that emerged during data analysis and aligns with the privacy strategy in the literature review. Privacy concerns for customer data is important for IT architects in various business units. Due regulatory compliance, IT architects must account for privacy laws in their strategy to adopt cloud computing services. IT architects can address privacy concerns by understanding privacy laws pertaining to their industry, limiting secondary usage of company data, and understanding trans-border data laws pertaining to data being shared by a cloud service provider and a subcontractor.

Privacy concerns is an external factor that can have an impact on PEOU or PU in the behavioral intent to adopt cloud computing services. Information stated by participants and reviewed in company documents supports privacy concerns as negative impact on PEOU and PU. Implementing certain privacy measures is not easy and has a negative impact on PEOU. Additionally, PU is impacted negatively because a system is not considered useful if customer privacy is not maintained. Liu, Shan, and Pigneur (2016) conducted research to determine if the PEOU and PU constructs had a positive impact on participants behavioral intention to utilize a mobile application when privacy was a concern. Liu et al. (2016) indicated that privacy concerns had a negative impact on PEOU and PU in a user's decision to utilize a new mobile application. Similar to the above mentioned research, the intention to adopt cloud computing services is based on privacy concerns impacting PEOU and PU. In both studies, privacy concerns had a negative impact on PEOU but in the previous study there was a positive impact on PU in the behavioral intention to use a new technology.

Service level agreements. Service level agreements was a theme that emerged during data analysis and aligns with the availability strategy in the literature review. IT architects and key stakeholders must align concerning service level agreements and guidelines for the company to follow when negotiating cloud computing services contracts. IT architects must understand the needs of their respective business units to determine how the needs may be met while staying within the company directive. Therefore, IT architects must become familiar with techniques to improve system availability in order to negotiate specific terms in a cloud computing services contract.

Service level agreements was a concern mentioned by three participants. Additionally, four company documents referenced service level agreements related to cloud computing services. Participants 1, 3, and 4 discussed company policy and service level agreements. IT architects can use Service level agreements to remediate their concerns for security, data availability and integrity, and privacy. Furthermore, cloud service providers and cloud services customers must have a clear understanding of service level agreements. The statement of work and service level agreement must outline security policies for the cloud service provider and the cloud services customer. If clear agreements are not met, both parties may inadvertently create a security vulnerability.

Participants 1 and 4 discussed the company's internal contract process. The internal contract process is negotiated by the sourcing and procurement department within the company. Although IT architects do not lead the contract process but they are considered subject matter experts for their respective business units and have an opportunity to provide feedback. Participant 1 discussed adding a system availability

table to cloud service contracts. Adding a system availability table to cloud service contracts enforces availability agreements and requires the vendor to provide a discount if certain system uptime thresholds are not met (see Table 8).

Table 8

Systems Availability for Service Level Agreement

System Availability (Monthly)	Service Level Credit (% of Monthly Fees)
99.8% - 98%	10%
97.99% - 96%	25%
95.99% - 94%	50%
Below 94%	100%

Participants 1, 3, and 4 discussed other benefits of a well written service level agreement. A well written service level agreement requires a cloud service provider to meet specific parameters concerning security, data availability and integrity, and privacy. Additionally, a previous study conducted by Wei et al. (2015) related data availability and integrity with the inability of a cloud service provider to provide a highly secure architecture platform caused some cloud computing services migrations to pause.

Participants 1, 3, and 4 discussed privacy concerns from a security breach. If the breach is caused by cloud service provider negligence, the provider is generally required to carry indemnity insurance upward to $10 million dollars. The cloud indemnity policy should have a designated multiplier of the agreed contract value. If customer data is breached, cloud service providers are usually required to provide credit monitoring for all business clients impacted. If the breach is caused by the customer, normal company

guidelines are followed for business clients. The question of breach ownership is resolved by routine reviews of audit logs as written in the security section of the service level agreement.

In summary, service level agreements was a theme that emerged during data analysis and aligns with the availability strategy in the literature review. Service level agreements are important part of the contract negotiations in the adoption of cloud computing services. Service level agreements in contract outline what is expected from the cloud service provider and what is required of the customer. A clear and defined service level agreement can help mitigate concerns for security, data availability and integrity, and privacy in the adoption of cloud computing services. Finally, service level agreements should contain an agreement to determine system level availability and discounts the availability criteria is not met.

Service level agreements is an external factor that can have an impact on PEOU or PU in the behavioral intent to adopt cloud computing services. Information stated by participants and reviewed in company documents supports service level agreements as a positive impact on PEOU and PU. Writing a clear and concise service level agreement with specific parameters concerning security, availability, and privacy for a cloud solution is complex and considered negative impact on PEOU. However, understanding the service levels based on business requirements for the cloud solution is considered positive impact to PU in the adoption of cloud computing services. A well-defined service level agreement will ensure the best solutions is delivered for the business unit. Fedorko, Bacik, and Gavurova (2018) used the TAM to explore if availability and quality

concerns impacted PEOU and PU in a participant's behavioral intent to use a new e-commerce website. Researchers in the study concluded that system availability and quality had a positive impact on PEOU and PU in the behavioral intent to use a new e-commerce site. In both studies, PU is considered a positive impact on the behavioral intent to adopt a new technology. However, this study concluded that PEOU was impacted negatively because service level agreements are difficult to negotiate, but are needed to enforce security, availability, and privacy standards.

Applications to Professional Practice

This research is meaningful to the adoption of cloud computing services in many ways. The main objective of the study was to explore participants' views concerning strategies used by IT architects when adopting cloud computing services. The adoption of cloud computing services is an increasing concern to IT architects and the IT industry in general (Raza et al., 2015). The findings of this study aligned with the TAM in aspects to the perceived ease of use and perceived usefulness in the evaluation process of adopting cloud computing services as a new technology (Aharony, 2015; Davis, 1986). Strategies to adopt cloud computing services are viewed as both a technology offering and business alternative to on-premise solutions by streamlining business processes and adding agility (Iyer et al., 2013). Additionally, Jede and Teuteberg (2016) indicated that cloud computing services emerged as an area of interest in business, because of ideas such as pay as you go services. With a simplified pay as you go usage policy, the adoption of cloud computing services offers adopters capabilities such as barebones infrastructure,

development environments as well as full software packages with minimal investments by consumers.

IT architects may enhance business value when making decisions concerning business processes for their respective business units by leveraging cloud computing services (Palos-Sanchez, Arenas-Marquez, & Aguayo-Camacho, 2017). Almost all of the participants of this research study indicated that using cloud computing services could reduce dependency on IT technical staff and on-premise infrastructure. Additionally, the data collected indicated that IT architects may start using cloud computing services for noncritical business processes. The strategic plan to move non-core processes to the cloud is consistent with information proved by previous research. Wang et al. (2016) explained the third step in a successful cloud computing services implementation is to start small by moving noncritical processes first to make sure the solution is stable and build confidence in employee utilization.

The increased agility offered by cloud computing services enables IT architects to deploy computational tools rapidly and respond more quickly to changing market needs (Oliveira et al., 2014; Tarmidi et al., 2014). Furthermore, some IT architects view cloud computing services as a technology offering and a business alternative, but their reasons for adopting cloud computing services is driven more by economic rationale than by technology justifications. Additionally, IT architects view cloud computing services as a merger of state of the art concepts like virtualization, server consolidation, interoperability and dynamic central processing unit (CPU) provisioning (Iyer et al.,

2013). Participant 6 stated the time to market for delivering a solution for their respective business unit improved with utilizing cloud computing services.

As a continuation of the business aspect, participants indicated that leadership focus shifted from capital expenditures to operational expenditures. The information provided by the participants was in alignment with a previous study. Carcary et al. (2014) indicated if cloud computing services are embraced, the upfront cost issue is reduced or removed. IT architects no longer have to buy IT assets, but IT architects can rent or lease IT assets from cloud computing service providers and consume the IT assets in a utility-based model when needed (Ratten, 2015). When a customer does not require IT services anymore, IT architects can discontinue the usage of the service with the cloud service provider to optimize cost. Additionally, the scalability and flexibility of cloud-based solutions allow IT architects the ability to fine tune solutions for the best return on investment. Participants 2 and 5 discussed the scalability to increase compute power during high claims times, but the flexibility to shrink back to normal compacity after the peak claims season. All participants in this study mentioned leveraging various strategies to adopt cloud computing services lowered business costs.

In addition to the praise for flexibility and scalability, participants indicated a concern for vendor lock-in. Gholami et al. (2016) indicated that customizing application programming interfaces to a particular cloud service provider is not recommended to prevent vendor lock-in. Because in doing so, a compatibility situation could occur if a cloud services customer decides to change cloud services provider. All participants of this study mentioned vendor lock-in as a major concern for portability and advised

against going full customization for a particular cloud service provider. As IT architects understand these strategies, the results of this study may assist IT architects in developing effective strategies to adopt cloud computing services for their respective business units.

Implications for Social Change

The implication for positive social change includes the impact from a business perspective and an environmental perspective. The use of cloud computing services is viewed as business agility through the efficiency of scaling IT resources (Oliveira et al., 2014). Participant 6 discussed the use of cloud computing services as a positive for his business unit because the business could switch SaaS vendors as needed. However, Participant 2 discussed impact to the business perspective because of lower upfront cost, on demand access to IT resources, lower operating cost, scalability, and mobility. With lower upfront costs, IT architects within companies can convert IT resources from a capital expense to an operational expense.

Carcary et al. (2014) determined if the use of cloud computing services is embraced, the upfront cost issue is reduced or removed. Additionally, Participant 1 discussed the efficiency of using cloud computing services over traditional IT. Furthermore, Participant 1 indicated the traditional IT model is designed around the rule of business units paying for hardware to address peak processing which means the same hardware may sit idle during nonpeak processing time. Avram (2014) and Oliveira et al. (2014) indicated the adoption of cloud computing services allows an IT architect to reliably scale IT resources up or down depending on business need and leads to a pay per use costing model similar to utilities.

The adoption of cloud computing services allows IT architects in an insurance company to become environmentally friendly. Participant 5 discussed the possibility of reducing electricity usage in the company data center because less servers will reside on-premise versus the cloud. Carbon emissions may be reduced if IT architects in an insurance company utilize a multitenant cloud solution versus a brick and mortar data center. For example, Google's data center consumes 1120 GWh equating to $67 million dollars annually and Microsoft consumes 600 GWH equating to $36 million dollars annually. In fact, generating 100 MWh in the U.S will emit 50 tons of carbon emissions (Gu et al., 2018). IT architects employed in small organizations with 100 or less users could reduce carbon emissions by 90% by simply adopting a cloud based email hosting. Therefore, IT architects in an insurance company can contribute positively to social change by reducing carbon emissions.

Adoption of cloud computing services has been beneficial in the communication filed allowing communication between companies and families thousands of miles apart. Companies can utilize meeting and collaborative tools such as Skype, WebEx, Google Docs, and Office 365 (Carcary et al., 2014). Additionally, the adoption of cloud computing services benefits public services such as educations, healthcare, and law enforcement (Park et al., 2016). Researchers and IT architects could utilize the findings from this study to develop a greater understanding of effective strategies to use when adopting cloud computing services.

Recommendations for Action

IT architects should consider reviewing the strategies in the first and second theme before starting an adoption of cloud computing services. The first and second themes are considered effective strategies to adopt cloud computing services. IT architects should start reviewing effective strategies to adopt cloud computing services to sustain productivity, growth, and competitive advantage (Avram, 2014). If strategies do not exist within an organization, IT architects should research the most effective strategies to adopt cloud computing services for the organization. If IT architects decide to execute a strategy to adopt cloud computing services, the IT architect should consider assessing the proposed strategies against generally known effective cloud adoption strategies. Additionally, IT architects should evaluate financial plans and budgets to allocate funding to support strategies to adopt cloud computing services. Furthermore, IT architects should align their strategies with key business initiatives for the company.

Results from this study are valuable to researchers, IT leaders, IT architects, and IT services consumers. The application of an effective strategy to adopt cloud computing services may enable IT architects to utilize strategic procedures to adopt cloud computing services and transform processes for their respective business unit. Furthermore, all company stakeholders involved in key business deliverables may be interested in the findings of this study. Additionally, understanding the results of this study may be particularly beneficial to current IT architects, by uncovering various strategies used by IT architects to adopt cloud computing services. I will distribute the results of the study

through scholarly and business journals. Additionally, I will socialize the results of this study with IT leaders within my company.

Recommendations for Further Study

The results from this study warrant further exploration of strategies used by IT architects when adopting cloud computing services for their respective business unit to sustain productivity, growth, and competitive advantage (Avram, 2014). The following are my recommendations for further research. First, the findings of this study warrant exploration of strategies used to adopt cloud computing services from the view of the business and not just technology. Second, this study was focused in the Illinois area and I recommend expanding the study to IT architects in other geographic locations. Third, I suggest performing the study with a larger sample size or including multiple insurance companies. Furthermore, I propose conducting the study across industries and not limiting the study to insurance. Insurance companies must comply with SOX, PII, PCI-DSS, and HIPAA which affect certain decisions concerning security and data. Fourth, the findings of this study warrant additional exploration to study critical strategies for all businesses to explore factors to measure the effectiveness of different strategies used to adopt cloud computing services. Fifth, I recommend assessing the strategies used to adopt cloud computing services against a company's key business initiatives because leadership within each company will have different business directives based on key performance indicators.

Future research may address the issue of having limited company documents to review. By having more company documents to review, I could have used the documents

to add additional information or context to the study. Additionally, I could have used the additional documentation to determine the effectiveness of current strategies or issues when adopting cloud computing services. Further research may also address the limitation of this study related to the inclusion of only IT architects. The addition of IT Managers may have provided a different business perspective. Additionally, future research may address the population size limitation of this study by expanding the geographical boundaries of the population sample.

Reflections

The pursuit of obtaining a Doctorate degree is demanding, but how demanding was not understood until I started the process. In my mind, obtaining a Doctorate in Information Technology was an extension of my Masters in Information Technology, but I was wrong. I grossly underestimated the time, effort, and sacrifices needed to achieve such a goal. I now understand the concept of all but dissertation (ABD) because getting through the coursework was the easy part, but maintaining focus and completing the dissertation has been hard. Additionally, I understand why so many people take a leave of absence from work when they are in the dissertation stage.

I chose to research the adoption of cloud computing services within an insurance company because my company was starting to adopt cloud computing services as an alternative for our data centers. I work for an insurance company and we have various business, operational, and technology areas requiring different aspects of cloud computing services. Most employees in my company use the cloud buzz word, but do not fully understand cloud computing services. Some of our IT architects retired their on-

premise solutions for SaaS based solutions, but as a company we did not have an overall plan for cloud computing services adoption. Because my company business units are so diverse, I felt a study of my company would help me understand strategies to adopt cloud computing services. Additionally, the information contained in this study may be beneficial to other insurance companies or any company starting their journey to adopt cloud computing services.

The participants in this exploratory case study provided knowledge regarding methods they used to adopt cloud computing services. I felt that using semistructured interview questions followed by probing questions would allow me to gather additional information from each participant. Furthermore, semistructured questions in a conversational format allowed participants to feel at ease and speak freely. Participants were eager to share their thoughts concerning their strategies and concerns for adopting cloud computing services. I also gained valuable information from participants pertaining to company initiatives, most effective strategy, least effective strategy, and various concerns when adopting cloud computing services. Because I work in a different technology area and my technology platform was not slated for cloud adoption, I did not previously talk to the participants about cloud computing services adoption. Furthermore, the lack of interactions with the participants before this study assisted me with avoiding biases.

Summary and Study Conclusions

I used this exploratory case study to explore the attitudes and opinions of participants about strategies used by IT architects when adopting cloud computing

services for their respective business units. Seven participants from an insurance company located in Illinois participated in the study. Each participant had the authority to impact decisions concerning strategies for adopting cloud computing services for their respective business unit. Data analysis consisted of using NVivo 12, a qualitative analysis software tool. I also used Microsoft Excel to categorize documents from the company intranet. I conducted member checking to confirm the responses of the interview recordings. The use of member checking reduced my risk of misunderstanding of information provided by each participant. I achieved data saturation when there were no new themes emerging.

After collecting and analyzing data, four main themes emerged from the data, including (a) strategies to adopt cloud computing services, (b) strategies to adopt cloud services models, (c) strategies to adopt cloud computing models, and (d) concerns affecting strategies to adopt cloud computing services. My findings indicated when there is not a clear overarching strategy in place to adopt cloud computing services, IT architects may face more challenges in adopting cloud computing services and meeting profitability, sustainability, and strategic goals. The findings also indicated that IT architects should understand the various offerings provided by cloud service providers to determine an effective strategy to address any concerns preventing the success of adopting cloud computing services.

References

Abbas, A., Bilal, K., Zhang, L., & Khan, S. (2015). A cloud based health insurance plan recommendation system: A user centered approach. *Future Generation Computer Systems, 43*, 99-109. doi:10.1016/j.future.2014.08.010

Abdullah, M., Iqbal, W., & Erradi, A. (2019). Unsupervised learning approach for web application auto-decomposition into microservices. *Journal of Systems & Software, 151*, 243-257. doi:10.1016/j.jss.2019.02.031

Adhikari, M., Nandy, S., & Amgoth, T. (2019). Meta heuristic-based task deployment mechanism for load balancing in IaaS cloud. *Journal of Network & Computer Applications, 128*, 64-77. doi:10.1016/j.jnca.2018.12.010

Aharony, N. (2014). Cloud computing: information professionals' and educational technology experts' perspectives. *Library Hi Tech, 32*(4), 645-666. doi:10.1108/LHT-02-2014-0024

Aharony, N. (2015). An exploratory study on factors affecting the adoption of cloud computing by information professionals. *The Electronic Library, 33*(2), 308. doi:10.1108/EL-09-2013-0163

Ajodhia-Andrews, A. (2016). Reflexively conducting research with ethnically diverse children with disabilities. *The Qualitative Report, 21*(2), 252-287. Retrieved from http://nsuworks.nova.edu/tqr/vol21/iss2/6

Akar, E., & Mardiyan, S. (2016). Analyzing factors affecting the adoption of cloud computing: A case of Turkey. *Transactions on Internet & Information Systems, 10*(1), 18-37. doi:10.3837/tiis.2016.01.002

Akman, I., & Mishra, A. (2015). Sector diversity in green information technology practices: technology acceptance model perspective. *Computers in Human Behavior, 49*, 477-486. doi:10.1016/j.chb.2015.03.009

Alfaro, I., & Watson-Manheim, M. (2015). Social media: A technology that needs no support from it...yet. *Journal of Computer Information Systems, 55*(3), 38-45. doi:10.1080/08874417.2015.11645770

Ali, M., Khan, S. U., & Vasilakos, A. V. (2015). Security in cloud computing: Opportunities and challenges. *Information Sciences, 305*, 357-383. doi:10.1016/j.ins.2015.01.025

Ali, O., Soar, J., & Yong, J. (2016). An investigation of the challenges and issues influencing the adoption of cloud computing in Australian regional municipal governments. *Journal of Information Security and Applications, 27*, 19-34. doi:10.1016/j.jisa.2015.11.006

Alkhuraiji, A., Liu, S., Oderanti, F. O., Annansingh, F., & Pan, J. (2014). Knowledge network modelling to support decision-making for strategic intervention in IT project-oriented change management. *Journal of Decision Systems, 23*(3), 285-302. doi:10.1080/12460125.2014.886499

Almamy, T., Taina, S., Airi, S., Erkki, S., & Yue, D. (2015). The role of trust in enhancing Internet use in a high-risk society. *Journal of Systems and Information Technology*, (2), 141. doi:10.1108/JSIT-09-2014-0066

Almarashdeh, I., & Alsmadi, M. K. (2017). How to make them use it? Citizens acceptance of M-government. *Applied Computing & Informatics, 13*(2), 194. doi:10.1016/j.aci.2017.04.001

Amadu, L., Muhammad, S. S., Mohammed, A. S., Owusu, G., & Lukman, S. (2018). Using technology acceptance model to measure the ese of social media for collaborative learning in Ghana. *Journal of Technology and Science Education, 8*(4), 321-336. doi:10.3926/jotse.383

Ambodo, B., Suryanto, S., & Sofyani, H. (2017). Testing of technology acceptance model on core banking system: A perspective on mandatory use. *Jurnal Dinamika Akuntansi, 9*, 11-22. doi:10.15294/jda.v9i1.12006

American Psychological Association. (2002). Ethical principles of psychologists and code of conduct. *American Psychologist, 57*(12), 1060-1073.

Ardagna, C. A., Asal, R., Damiani, E., & Quang Hieu, V. (2015). From security to assurance in the cloud: A survey. *ACM Computing Surveys, 48*(1), 1-50. doi:10.1145/2767005

Arsovski, S., Arsovski, Z., Stefanović, M., Tadić, D., & Aleksić, A. (2017). Organisational resilience in a cloud-based enterprise in a supply chain: a challenge for innovative SMEs. *International Journal of Computer Integrated Manufacturing, 30*(4-5), 409-419. doi:10.1080/0951192X.2015.1066860

Ashtari, S., & Eydgahi, A. (2017). Student perceptions of cloud applications effectiveness in higher education. *Journal of Computational Science, 23*, 173-180. doi:10.1016/j.jocs.2016.12.007

Avram, M. G. (2014). Advantages and challenges of adopting cloud computing from an enterprise perspective. *Procedia Technology*, *12*, 529-534. doi:10.1016/j.protcy.2013.12.525

Basahel, A., Yamin, M., & Drijan, A. (2016). Barriers to cloud computing adoption for SMEs in Saudi Arabia. *BVICAM's International Journal of Information Technology*, *8*(2), 1044-1048. Retrieved from http://www.bvicam.ac.in/bjit/downloads/pdf/issue16/11.pdf

Battleson, 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. doi:10.1057/ejis.2015.12

Bell, E. E. (2017). A narrative inquiry: A black male looking to teach. *The Qualitative Report*, *22*(4), 1137-1150. Retrieved from https://nsuworks.nova.edu/tqr/vol22/iss4/12

Bengtsson, M. (2016). How to plan and perform a qualitative study using content analysis. *Nursing Open*, *2*, 8-14. doi:10.1016/j.npls.2016.01.001

Bhadauria, R., Chaki, R., Chaki, N., & Sanyal, S. (2014). A survey on security issues in cloud computing. *Acta Technica Corviniensis - Bulletin of Engineering, 7*(4), 159-177. Retrieved from http://acta.fih.upt.ro/pdf/archive/ACTA-2014-4.pdf

Bhatiasevi, V. V., & Naglis, M. M. (2016). Investigating the structural relationship for the determinants of cloud computing adoption in education. *Education & Information Technologies, 21*(5), 1197-1223. doi:10.1007/s10639-015-9376-6

Bhattacherjee, A., & Park, S. C. (2014). Why end-users move to the cloud: A migration-theoretic analysis. *European Journal of Information Systems, 23*(3), 357-372. doi:10.1057/ejis.2013.1

Bildosola, I., Río-Belver, R., Cilleruelo, E., & Garechana, G. (2015). Design and implementation of a cloud computing adoption decision tool: Generating a cloud road. *PLoS One, 10*(7), e0134563. doi:10.1371/journal.pone.0134563

Botta, A., de Donato, W., Persico, V., & Pescapé, A. (2016). Integration of cloud computing and internet of things: A survey. *Future Generation Computer Systems, 56*, 684-700. doi:10.1016/j.future.2015.09.021

Budi, I., & Rafur, H. (2017). Analysis of success factors in the implementation of ERP system in research institute. *Journal of Theoretical & Applied Information Technology, 95*(12), 2830-2839. Retrieved from http://www.jatit.org/volumes/ninetyfive12.php

Cairney, P., & St Denny, E. (2015). Reviews of what is qualitative research and what is qualitative interviewing. *International Journal of Social Research Methodology, 18*(1), 117-125. doi:10.1080/13645579.2014.957434

Caldarelli, A., Ferri, L., & Maffei, M. (2017). Expected benefits and perceived risks of cloud computing: an investigation within an Italian setting. *Technology Analysis & Strategic Management, 29*(2), 167-180. doi:10.1080/09537325.2016.1210786

Carcary, M., Doherty, E., Conway, G., & McLaughlin, S. (2014). Cloud computing adoption readiness and benefit realization in Irish SMEs—An exploratory study. *Information Systems Management, 31*(4), 313-327. doi:10.1080/10580530.2014.958028

Castillo-Montoya, M. (2016). Preparing for interview research: The interview protocol refinement framework. *The Qualitative Report*, *21*(5), 811-831. Retrieved from https://nsuworks.nova.edu/tqr/vol21/iss5/2

Castleberry, A., & Nolen, A. (2018). Methodology matters: Thematic analysis of qualitative research data: Is it as easy as it sounds?. *Currents in Pharmacy Teaching and Learning*, doi:10.1016/j.cptl.2018.03.019

Chang, V., Kuo, Y., & Ramachandran, M. (2016). Cloud computing adoption framework: A security framework for business clouds. *Future Generation Computer Systems*, *57*, 24-41. doi:10.1016/j.future.2015.09.031

Changchit, C., & Chuchuen, C. (2018). Cloud computing: An examination of factors impacting users' adoption. *Journal of Computer Information Systems, 58*(1), 1-9. doi:10.1080/08874417.2016.1180651

Changthong, J., Manmart, L., & Vongprasert, C. (2014). Learning styles: Factors affecting information behavior of Thai youth. *LIBRES: Library and Information Science Research Electronic Journal*, *24*(1), 50-61. Retrieved from https://www.libres-ejournal.info/all-issues/volume-24-issue-1/

Chen, C., Xu, X., & Arpan, L. (2017). Between the technology acceptance model and sustainable energy technology acceptance model: Investigating smart meter acceptance in the United States. *Energy Research & Social Science, 25*, 93-104. doi:10.1016/j.erss.2016.12.011

Chen, H. C., & Lee, P. P. (2014). Enabling data integrity protection in regenerating-coding-based cloud storage: Theory and implementation. *IEEE Transactions on Parallel & Distributed Systems*, *25*(2), 407-416. doi:10.1109/TPDS.2013.164

Cohen, D. J., Keller, S. R., Hayes, G. R., Dorr, D. A., Ash, J. S., & Sittig, D. F. (2015). Developing a model for understanding patient collection of observations of daily living: A qualitative meta-synthesis of the project health design program. *Personal and Ubiquitous Computing, 19*(1), 91-102. doi:10.1007/s00779-014-0804-1

Coppolino, L., D'Antonio, S., Mazzeo, G., & Romano, L. (2017). Cloud security: Emerging threats and current solutions. *Computers & Electrical Engineering*, *59*, 126-140. doi:10.1016/j.compeleceng.2016.03.004

Cusack, B., & Ghazizadeh, E. (2016). Evaluating single sign-on security failure in cloud services. *Business Horizons*, *59*, 605-614. doi:10.1016/j.bushor.2016.08.002

Davidovic, V., Ilijevic, D., Luk, V., & Pogarcic, I. (2015). Private cloud computing and delegation of control. *Procedia Engineering*, *100*, 196-205. doi:10.1016/j.proeng.2015.01.358

Davis, F. D. (1986). *A technology acceptance model for empirically testing new end user information systems: Theory and results* (Doctoral dissertation). Massachusetts Institute of Technology. Retrieved from http://hdl.handle.net/1721.1/15192

Davis, F. D., Bagozzi, R. P., & Warshaw, P. R. (1989). User acceptance of computer technology: A comparison of two theoretical models. *Management Science, 35*, 982-1003. doi:10.1287/mnsc.35.8.982

Daylami, N. (2015). The origin and construct of cloud computing. *International Journal of the Academic Business World*, *9*(2), 39-45. Retrieved from http://jwpress.com/IJABW/Issues/IJABW-Fall-2015.pdf

DeFeo, D. J. (2013). Toward a model of purposeful participant inclusion: Examining deselection as a participant risk. *Qualitative Research Journal, 13*(3), 253-264. doi:10.1108/qrj-01-2013-0007

Dhasarathan, C., Thirumal, V., & Ponnurangam, D. (2017). A secure data privacy preservation for on-demand cloud service. *Journal of King Saud University - Engineering Sciences, 29(2),* 144-150. doi:10.1016/j.jksues.2015.12.002.

Dixon, C. S. (2015). Interviewing adolescent females in qualitative research. *The Qualitative Report, 20*(12), 2067-2077. Retrieved from http://nsuworks.nova.edu/tqr/vol20/iss12/12

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, 3*, 512-527. doi:10.1108/JSBED-05-2013-0069

Dowse, E. M., van der Riet, P., & Keatinge, D. R. (2014). A student's perspective of managing data collection in a complex qualitative study. *Nurse Researcher*, *22*(2), 34. doi:10.7748/nr.22.2.34.e1302

Durrani, U. K., Pita, Z., & Richardson, J. (2014). Coexistence of agile and SCM practices. *Journal of Systems and Information Technology*, *16*(1), 20-39. doi:10.1108/JSIT-09-2013-0045

El-Gazzar, R., Hustad, E., & Olsen, D. H. (2016). Understanding cloud computing adoption issues: A Delphi study approach. *Journal of Systems and Software*, *118*, 64-84. doi:10.1016/j.jss.2016.04.061.

Elo, S., Kääriäinen, M., Kanste, O., Pölkki, T., Polkki, T., Utriainen, K., & Kyngas, H. (2014). Qualitative content analysis: A focus on trustworthiness. *SAGE Open*, *4*(1), 1-10. doi:10.1177/2158244014522633

Esteban-Millat, I., Martínez-López, F. J., Pujol-Jover, M., Gázquez-Abad, J. C., & Alegret, A. (2018). An extension of the technology acceptance model for online learning environments. *Interactive Learning Environments*, *26*(7), 895-910. doi:10.1080/10494820.2017.1421560

Fedorko, I., Bacik, R., & Gavurova, B. (2018). Technology acceptance model in e-commerce segment. *Management & Marketing*, *13*(4), 1242-1256. doi:10.2478/mmcks-2018-0034

Fusch, P. I., & Ness, L. R. (2015). Are we there yet? Data saturation in qualitative research. *The Qualitative Report*, *20*, 1408. Retrieved from http://nsuworks.nova.edu/tqr/vol20/iss9/3

Gan, C. L., & Balakrishnan, V. (2014). Determinants of mobile wireless technology for promoting interactivity in lecture sessions: An empirical analysis. *Journal of Computing in Higher Education, 26*(2), 159-181. doi:10.1007/s12528-014-9082-1

Gangwar, H., & Date, H. (2016). Critical factors of cloud computing adoption in organizations: An empirical study. *Global Business Review*, *17*(4), 886-904. doi:10.1177/0972150916645692

Ganjikhah, A., Rabiee, A., Moghaddam, D. K., & Vahdat, D. (2017). Comparative analysis of bank's ATM and POS technologies by customers. *Independent Journal of Management & Production, 8*(3). 831-848. doi:10.14807/ijmp.v8i3.528

Garrison, G., Rebman, C. M., & Kim, S. H. (2018). An identification of factors motivating individuals' use of cloud-based services. *Journal of Computer Information Systems, 58*(1), 19-29. doi:10.1080/08874417.2016.1180653

Gashami, J. G., Chang, Y., Rho, J. J., & Park, M. (2016). Privacy concerns and benefits in SaaS adoption by individual users. *Information Development*, *32*(4), 837-852. doi:10.1177/0266666915571428

Gergen, K. J., Josselson, R., & Freeman, M. (2015). The promises of qualitative inquiry. *American Psychologist*, *70*, 1. doi:10.1037/a0038597

Gholami, M. F., Daneshgar, F., Low, G., & Beydoun, G. (2016). Cloud migration process—A survey, evaluation framework, and open challenges. *Journal of Systems and Software, 120*, 31-69. doi:10.1016/j.jss.2016.06.068

Ghorbel, A., Ghorbel, M., & Jmaiel, M. (2017). Privacy in cloud computing environments: A survey and research challenges. *Journal of Supercomputing*, *73*(6), 2763-2800. doi:10.1007/s11227-016-1953-y

Giray, G., & Tüzün, E. (2018). A systematic mapping study on the current status of total cost of ownership for information systems. *International Journal of Informatics Technologies, 11*(2), 131-145. doi:10.17671/gazibtd.327544

Golafshani, N. (2003). Understanding reliability and validity in qualitative research. *The Qualitative Report*, *8*(4), 597-606. Retrieved from https://nsuworks.nova.edu/tqr/vol8/iss4/6

Goutas, L., Sutanto, J., & Aldarbesti, H. (2016). The building blocks of a cloud strategy: Evidence from three SaaS providers. *Communications of the ACM*, *59*(1), 90-97. doi:10.1145/2756545

Grozev, N., & Buyya, R. (2014). Multi-cloud provisioning and load distribution for three-tier applications. *ACM Transactions on Autonomous and Adaptive Systems*, *9*(3), 13. doi:10.1145/2662112

Grozev, N., & Buyya, R. (2016). Regulations and latency-aware load distribution of web applications in Multi-Clouds. *Journal of Supercomputing*, *72*(8), 3261-3280. doi:10.1007/s11227-016-1735-6

Gu, C., Fan, L., Wu, W., Huang, H., & Jia, X. (2018). Greening cloud data centers in an economical way by energy trading with power grid. *Future Generation Computer Systems, 78,* 89-101. doi:10.1016/j.future.2016.12.029

Haegele, J. A., & Hodge, S. R. (2015). Quantitative methodology: A guide for emerging physical education and adapted physical education researchers. *Physical Educator, 72*, 59-75. doi:10.18666/tpe-2015-v72-i5-6133

Han, J., Li, Y., & Chen, W. (2019). A lightweight and privacy-preserving public cloud auditing scheme without bilinear pairings in smart cities. *Computer Standards & Interfaces, 62*, 84–97. doi:10.1016/j.csi.2018.08.004

Hassan, H., Nasir, M. M., Khairudin, N., & Adon, I. (2017). Factors influencing cloud computing adoption in small and medium enterprises. *Journal of Information and Communication Technology, 16*(1), 21-41. Retrieved from http://aisel.aisnet.org/pajais/vol9/iss3/3

Helia, V. N., Asri, V. I., Kusrini, E., & Miranda, S. (2018). Modified technology acceptance model for hospital information system evaluation - A case study. *MATEC Web of Conferences, 154*, 1101. doi:10.1051/matecconf/201815401101

Hersh, M. (2014). Science, technology and values: Promoting ethics and social responsibility. *AI & Society, 29*(2), 167-183. doi:10.1007/s00146-013-0473-z

Hew, J., Leong, L., Tan, G. W., Lee, V., & Ooi, K. (2018). Mobile social tourism shopping: A dual-stage analysis of a multi mediation model. *Tourism Management, 66*(1), 121-139. doi:10.1016/j.tourman.2017.10.005

Ho, S. M., Booth, C., & Ocasio-Velázquez, M. (2017). Trust or consequences? Causal effects of perceived risk and subjective norms on cloud technology adoption. *Computers & Security, 70*, 581-595. doi:10.1016/j.cose.2017.08.004

Hsu, H., & Wu, Y. (2017). Investigation of the effects of a nursing information system by using the technology acceptance model. *Computers Informatics Nursing, 35*(6), 315–322. doi:10.1097/CIN.0000000000000313

Hsu, P., Ray, S., & Li-Hsieh, Y. (2014). Examining cloud computing adoption intention, pricing mechanism, and deployment model. *International Journal of Information Management, 34*(4), 474-488. doi:10.1016/j.ijinfomgt.2014.04.006

Huang, Y. M. (2017). Exploring students' acceptance of team messaging services: The roles of social presence and motivation. *British Journal of Educational Technology, 48*(4), 1047-1061. doi:10.1111/bjet.12468

Iyer, E. K., Krishnan, A., Sareen, G., & Panda, T. (2013). Sectorial adoption analysis of cloud computing by examining the dissatisfier landscape. *Electronic Journal of Information Systems Evaluation*, *16*(3), 212-220. Retrieved from http://www.ejise.com/volume16/issue3/p211

Jede, A., & Teuteberg, F. (2016). Investigating preconditions for a financially advantageous cloud usage. *International Journal of Accounting and Information Management, 24*(2), 116-134. doi:10.1108/IJAIM-04-2015-0018

Jeganathan, S. (2019). Practical approaches to overcome security challenges in cloud computing: Part 2: Private cloud. *ISSA Journal*, *17*(1), 41-46. Retrieved from https://www.bluetoad.com/publication/?i=556006

Johnson, M. E., Brems, C., Hanson, B. L., Corey, S. L., Eldridge, G. D., & Mitchell, K. (2013). Conducting ethical research with correctional populations: Do researchers and IRB members know the federal regulations?. *Research Ethics, 10*, 6-16. doi:10.1177/1747016113494652

Juels, A., & Oprea, A. (2013). New approaches to security and availability for cloud data. *Communications of the ACM*, *56*(2), 64-73. doi:10.1145/2408776.2408793

Kang, Y., & Stasko, J. (2014). Characterizing the intelligence analysis process through a longitudinal field study: Implications for visual analytics. *Information Visualization, 13*(2), 134-158. doi:10.1177/1473871612468877

Karanasios, S., & Allen, D. (2014). Mobile technology in mobile work: Contradictions and congruencies in activity systems. *European Journal of Information Systems, 23*(5), 529-542. doi:10.1057/ejis.2014.20

Kaul, S., Sood, K., & Jain, A. (2017). Cloud computing and its emerging need: Advantages and issues. *International Journal of Advanced Research in Computer Science*, *8*(3), 618-624. doi:10.26483/ijarcs.v8i3.3064

Khan, A. (2017). Key characteristics of a container orchestration platform to enable a modern application. *IEEE Cloud Computing, 4*(5), 42-48. doi:10.1109/MCC.2017.4250933

Kim, J. (2015). Survey for sensor-cloud system from business process outsourcing perspective. *International Journal of Distributed Sensor Networks*, *11*(9), 917028. doi:10.1155/2015/917028

Kirkwood, A., & Price, L. (2013). Examining some assumptions and limitations of research on the effects of emerging technologies for teaching and learning in higher education: Examining assumptions and limitations of research. *British Journal of Educational Technology*, *44*, 536-543. doi:10.1111/bjet.12049

Koo, C. J., & Kim, J. (2015). Decision making for the adoption of cloud computing for sensor data: From the viewpoint of industrial security. *International Journal of Distributed Sensor Networks*, *11*(9), 581563. doi:10.1155/2015/581563

Kornbluh, M. (2015). Combatting challenges to establishing trustworthiness in qualitative research. *Qualitative Research in Psychology*, *12*(4), 397-414. doi:10.1080/14780887.2015.1021941

Kouatli, I. (2014). A comparative study of the evolution of vulnerabilities in IT systems and its relation to the new concept of cloud computing. *Journal of Management History, 20*(4), 409-433. doi:10.1108/JMH-02-2014-0018

Kung, L., Cegielski, C. G., & Kung, H. (2015). An integrated environmental perspective on software as a service adoption in manufacturing and retail firms. *Journal of Information Technology*, *30*(4), 352-363. doi:10.1057/jit.2015.14

Lal, P., & Bharadwaj, S. S. (2016). Understanding the impact of cloud-based services adoption on organizational flexibility. *Journal of Enterprise Information Management*, *29*(4), 566-588. doi:10.1108/JEIM-04-2015-0028

Larosiliere, G. D., & Carter, L. D. (2016). Using a fit-viability approach to explore the determinants of e-government maturity. *Journal of Computer Information Systems, 56*(4), 271-279. doi:10.1080/08874417.2016.1163995

Laumer, S., Maier, C., Eckhardt, A., & Weitzel, T. (2016). Work routines as an object of resistance during information systems implementations: Theoretical foundation and empirical evidence. *European Journal of Information Systems, 25*(4), 317-343. doi:10.1057/ejis.2016.1

Lawrence, J. E., & Tar, U. A. (2018). Factors that influence teachers' adoption and integration of ICT in teaching/learning process. *Educational Media International, 55*(1), 79-105. doi:10.1080/09523987.2018.1439712

Lee, N., Li, S., Shin, B., & Kwon, O. (2016). Social comparison, goal contagion, and adoption of innovative information technology. *Journal of Computer Information Systems*, *56*(2), 127-136. doi:10.1080/08874417.2016.1117374

Lee, Y. C. (2016). Why do people adopt cloud services? Gender differences. *Social Science Information*, *55*(1), 78-93. doi:10.1177/0539018415609174

Li, G., & Wei, M. (2014). Everything-as-a-service platform for on-demand virtual enterprises. *Information Systems Frontiers*, *16*(3), 435-452. doi:10.1007/s10796-012-9351-3

Lian, J. W., Yen, D. C., & Wang, Y. T. (2014). An exploratory study to understand the critical factors affecting the decision to adopt cloud computing in Taiwan hospital. *International Journal of Information Management*, *34*(1), 28-36. doi:10.1016/j.ijinfomgt.2013.09.004

Linthicum, D. S. (2017). Cloud-native applications and cloud migration: The good, the bad, and the points between. *IEEE Cloud Computing*, *4*(5), 12-14. doi:10.1109/MCC.2017.4250932

Liu, H. (2013). Big data drives cloud adoption in enterprise. *IEEE Internet Computing*, *17*(4), 68-71. doi:10.1109/MIC.2013.63

Liu, Z., Shan, J., & Pigneur, Y. (2016). The role of personalized services and control: An empirical evaluation of privacy calculus and technology acceptance model in the mobile context. *Journal of Information Privacy & Security, 12*(3), 123-144. doi:10.1080/15536548.2016.1206757

López García, Á., Fernández del Castillo, E., & Orviz Fernández, P. (2016). Standards for enabling heterogeneous IaaS cloud federations. *Computer Standards & Interfaces*, *47*, 19-23. doi:10.1016/j.csi.2016.02.002

Loukis, E., Janssen, M., & Mintchev, I. (2019). Determinants of software-as-a-service benefits and impact on firm performance. *Decision Support Systems, 117*, 38-47. doi:10.1016/j.dss.2018.12.005

Lu, X., Yin, J., Xiong, N. N., Deng, S., He, G., & Yu, H. (2016). JTangCMS: An efficient monitoring system for cloud platforms. *Information Sciences, 370-371*, 402-423. doi:10.1016/j.ins.2016.06.009

Lub, V. (2015). Validity in qualitative evaluation: Linking purposes, paradigms, and perspectives. *International Journal of Qualitative Methods, 14*, 1-8. doi:10.1177/1609406915621406

Mac-Anigboro, O., & Usoro, A. (2015). Usability in ensuring a successful post implementation adoption of cloud enterprise resource planning systems: A proposed research. *Computing and Information Systems, 19*(2), 1-10. Retrieved from https://www.highbeam.com/doc/1G1-471554575

Maqueira-Marín, J. M., Bruque-Cámara, S., & Minguela-Rata, B. (2017). Environment determinants in business adoption of cloud computing. *Industrial Management & Data Systems, 117*(1), 228-246. doi:10.1108/IMDS-11-2015-0468

Mark, S., Dietmar, N., Werner, W., Gerold, W., & Michael A., E. (2018). Factors influencing the organizational adoption of cloud computing: a survey among cloud workers. *International Journal of Information Systems and Project Management, 6*(1), 5-23. doi:10.12821/ijispm060101

Mazerolle, S. M., Burton, L., & Cotrufo, R. J. (2015). The experiences of female athletic trainers in the role of the head athletic trainer. *Journal of Athletic Training, 50*(1), 71-81. doi:10.4085/1062-6050-49.3.50

Melin, U., & Axelsson, K. (2016). Action in action research. *Journal of Systems and Information Technology, 18*(2), 118-147. doi:10.1108/JSIT-10-2015-0074

Mendonça, J., Andrade, E., Endo, P. T., & Lima, R. (2019). Disaster recovery solutions for IT systems: A Systematic mapping study. *The Journal of Systems & Software, 149*, 511-530. doi:10.1016/j.jss.2018.12.023

Method of cloud system disaster recovery based on “Infrastructure as a code” concept. (2018). *2018 14th International Conference on Advanced Trends in Radioelecrtronics, Telecommunications and Computer Engineering (TCSET), Advanced Trends in Radioelecrtronics, Telecommunications and Computer Engineering (TCSET), 2018 14th International Conference On*, 1139. doi:10.1109/TCSET.2018.8336395

Middleton, C., Scheepers, R., & Tuunainen, V. K. (2014). When mobile is the norm: Researching mobile information systems and mobility as post-adoption phenomena. *European Journal of Information Systems, 23*(5), 503-512. doi:10.1057/ejis.2014.21

Mohammed, F., Ibrahim, O., Nilashi, M., & Alzurqa, E. (2016). Cloud computing adoption model for e-government implementation. *Information Development*, *33*(3), 303-323. doi:10.1177/0266666916656033

Moustakas, C. E. (1994). *Phenomenological research methods*. Thousand Oaks, CA: Sage Publications.

Muller Mirza, N., & Perret-Clermont, A. (2016). "Are you really ready to change?" an actor-oriented perspective on a farmers training setting in Madagascar. *European Journal of Psychology of Education, 31*(1), 79-93. doi:10.1007/s10212-014-0238-1

Neuman, D. (2014). Qualitative research in educational communications and technology: A brief introduction to principles and procedures. *Journal of Computing in Higher Education*, *26*(1), 69-86. doi:10.1007/s12528-014-9078-x

Novkovic, G., & Korkut, T. (2017). Software and data regulatory compliance in the cloud. *Software Quality Professional*, *20*(1), 4. Retrieved from http://asq.org/pub/sqp/past/vol20_issue1/index.html

Ohmann, C., Canham, S., Danielyan, E., Robertshaw, S., Legré, Y., Clivio, L., & Demotes, J. (2015). Cloud computing and clinical trials: Report from an ECRIN workshop. *Trials*, *16*(1), 1-4. doi:10.1186/s13063-015-0835-6

Okai, S., Uddin, M., Arshad, A., Alsaqour, R., & Shah, A. (2014). Cloud computing adoption model for universities to increase ICT proficiency. *SAGE Open*, *4*(3), 2158244014546461. doi:10.1177/2158244014546461

Olaronke, I., & Oluwaseun, O. (2016). Big data in healthcare: Prospects, challenges and resolutions. *2016 Future Technologies Conference (FTC),* San Francisco, CA, 1152-1157. doi:10.1109/FTC.2016.7821747

Oliveira, T., Thomas, M., & Espadanal, M. (2014). Assessing the determinants of cloud computing adoption: An analysis of the manufacturing and services sectors. *Information & Management, 51*(5), 497-510. doi:10.1016/j.im.2014.03.006

Opara-Martins, J., Sahandi, R., & Tian, F. (2016). Critical analysis of vendor lock-in and its impact on cloud computing migration: A business perspective. *Journal of Cloud Computing*, *5*(1), 1. doi:10.1186/s13677-016-0054-z

O'Reilly, M., & Parker, N. (2012). 'Unsatisfactory saturation': A critical exploration of the notion of saturated sample sizes in qualitative research. *Qualitative Research*, *13*, 190-197. doi:1468794112446106.

Ouahman, A. A. (2014). Security and privacy issues in cloud computing. *Journal of Defense Resources Management, 5*(2), 99-108. Retrieved from http://journal.dresmara.ro/issues/volume5_issue2/09_bibo.pdf

Oye, C., Sorensen, N. O., & Glasdam, S. (2016). Qualitative research ethics on the spot: Not only on the desktop. *Nursing Ethics*, *23*(4), 455-464. doi:10.1177/0969733014567023

Pakath, R. (2015). Competing on the cloud: A review and synthesis of potential benefits and possible pitfalls. *Journal of Organizational Computing & Electronic Commerce*, *25*(1), 1-27. doi:10.1080/10919392.2015.990771

Palinkas, L. A., Horwitz, S. M., Green, C. A., Wisdom, J. P., Duan, N., & Hoagwood, K. (2015). Purposeful sampling for qualitative data collection and analysis in mixed method implementation research. *Administration and Policy in Mental Health and Mental Health Services Research, 42*(5), 533-544. doi:10.1007/s10488-013-0528-y

Pallant, A., McIntyre, C., & Stephens, A. L. (2016). Transforming undergraduate research opportunities using telepresence. *Journal of Geoscience Education, 64*(2), 138-146. doi:10.5408/15-118.1

Palos-Sanchez, P. R., Arenas-Marquez, F. J., & Aguayo-Camacho, M. (2017). Cloud computing (SaaS) adoption as a strategic technology: Results of an empirical study. *Mobile Information Systems*, 2017. doi: 10.1155/2017/2536040

Palvia, P., Baqir, N., & Nemati, H. (2018). ICT for socio-economic development: A citizens' perspective. *Information & Management, 55*(2), 160-176. doi:10.1016/j.im.2017.05.003

Pappa, I. C., Iliopoulos, C., & Massouras, T. (2018). What determines the acceptance and use of electronic traceability systems in agri-food supply chains?. Journal of Rural Studies, 58, 123-135. doi:10.1016/j.jrurstud.2018.01.001

Park, E., & Kim, K. J. (2014). An integrated adoption model of mobile cloud services: Exploration of key determinants and extension of technology acceptance model. *Telematics and Informatics, 31*(3), 376-385. doi:10.1016/j.tele.2013.11.008

Park, S., Im, H., & Noh, K. (2016). A study on factors affecting the adoption of LTE mobile communication service: The case of South Korea. *Wireless Personal Communications, 86*(1), 217-237. doi:10.1007/s11277-015-2802-7

Paulus, T. M., Lester, J. N., & Britt, V. G. (2013). Constructing hopes and fears around technology: A discourse analysis of introductory qualitative research texts. *Qualitative Inquiry, 19*(9), 639-651. doi:10.1177/1077800413500929

Pedro, R. P., Francisco, J. A., & Mariano, A. (2017). Cloud computing (SaaS) adoption as a strategic technology: Results of an empirical study. *Mobile Information Systems, 2017*, 1-20. doi:10.1155/2017/2536040

Peng, G. C. A., & Gala, C. (2014). Cloud ERP: A new dilemma to modern organisations?. *Journal of Computer Information Systems, 54*(4), 22-30. doi:10.1080/08874417.2014.11645719

Petac, E., & Petac, A. (2016). The challenge of private cloud for the digital business. *Ovidius University Annals, Series Economic Sciences, 16*(1), 373-379. Retrieved from https://doaj.org/article/0d157a543d564481ad1dc849b007a688

Phaphoom, N., Wang, X., Samuel, S., Helmer, S., & Abrahamsson, P. (2015). A survey study on major technical barriers affecting the decision to adopt cloud services. *Journal of Systems & Software, 103*, 167-181. doi:10.1016/j.jss.2015.02.002

Piesse, D. (2014). Keyless signature infrastructure for insurance cyber liability. *Journal of The Insurance Institute of India, 1*(3), 27-31. Retrieved from http://www.coi.org.in//downloads/NewsLetter_SWF%202013-2014/Journal%20Jan-Mar%202014/index.html#p=2

Qian, R., & Palvia, P. (2013). Towards an understanding of cloud computing's impact on organizational IT strategy. *Journal of Information Technology Case and Application Research, 15*(4), 34-54. doi:10.1080/15228053.2013.10845727

Rahi, S., Ghani, M., & Alnaser, F. (2017). Predicting customer's intentions to use internet banking: the role of technology acceptance model (TAM) in e-banking. *Management Science Letters, 7*(11), 513-524. doi:10.5267/j.msl.2017.8.004

Rasheed, H. (2014). Data and infrastructure security auditing in cloud computing environments. *International Journal of Information Management, 34*(3), 364-368. doi:10.1016/j.ijinfomgt.2013.11.002

Rasouli, M. R., Trienekens, J. J. M., Kusters, R. J., & Grefen, P. W. P. J. (2016). Information governance requirements in dynamic business networking. *Industrial Management & Data Systems, 116*(7), 1356-1379. doi:10.1108/IMDS-06-2015-0260

Ratten, V. (2015). International consumer attitudes toward cloud computing: A social cognitive theory and technology acceptance model perspective. *Thunderbird International Business Review, 57*(3), 217-228. doi:10.1002/tie.21692

Ray, D. (2016). Cloud adoption decisions: Benefitting from an integrated perspective. *Electronic Journal of Information Systems Evaluation, 19*(1), 3-22. Retrieved from http://www.ejise.com/volume19/issue1/p3

Raza, M. H., Adenola, A. F., Nafarieh, A., & Robertson, W. (2015). The slow adoption of cloud computing and it workforce. *Procedia Computer Science, 52,* 1114-1119. doi:10.1016/j.procs.2015.05.128

Razmak, J., & Bélanger, C. (2018). Using the technology acceptance model to predict patient attitude toward personal health records in regional communities. *Information Technology & People, 31*(2), 306. doi:10.1108/ITP-07-2016-0160

Rehman, Z., Hussain, O. K., & Hussain, F. K. (2015). User-side cloud service management: State-of-the-art and future directions. *Journal of Network and Computer Applications, 55,* 108-122. doi:10.1016/j.jnca.2015.05.007

Ribas, M., Furtado, C., de Souza, J. N., Barroso, G. C., Moura, A., Lima, A. S., & Sousa, F. R. (2015). A Petri net-based decision-making framework for assessing cloud services adoption: The use of spot instances for cost reduction. *Journal of Network and Computer Applications, 57,* 102-118. doi:10.1016/j.jnca.2015.07.002

Ring, T. (2015). Cloud security fears: Fact or FUD?. *Network Security, 2015*(7), 10-14. doi:10.1016/S1353-4858(15)30058-1

Riungu-kalliosaari, L., Taipale, O., Smolander, K., & Richardson, I. (2016). Adoption and use of cloud-based testing in practice. *Software Quality Journal, 24*(2), 337-364. doi:10.1007/s11219-014-9256-0

Robinson, O. C. (2014). Sampling in interview-based qualitative research: A theoretical and practical guide. *Qualitative Research in Psychology*, *11*(1), 25-41. doi:10.1080/14780887.2013.801543

Rogers, E. (2003). *Diffusion of Innovations* (5th ed.). New York, NY: The Free Press.

Rong, C., Nguyen, S. T., & Jaatun, M. G. (2013). Beyond lightning: A survey on security challenges in cloud computing. *Computers & Electrical Engineering*, *39*(1), 47-54. doi:10.1016/j.compeleceng.2012.04.015

Rubóczki, E. S., & Rajnai, Z. (2015). Moving towards cloud security. *Interdisciplinary Description of Complex Systems*, *13*(1), 9-14. doi:10.7906/indecs.13.1.2

Ruoning, Q., & Palvia, P. (2013). Towards an understanding of cloud computing's impact on organization it strategy. *Journal of Information Technology Case and Application Research*, *15*(4), 34-54. doi:10.1080/15228053.2013.10845727

Sabi, H. M., Uzoka, F. E., Langmia, K., & Njeh, F. N. (2016). Conceptualizing a model for adoption of cloud computing in education. *International Journal of Information Management*, *36*(2), 183-191. doi:10.1016/j.ijinfomgt.2015.11.010

Saeid, E., Yousef, M., Afsaneh, K., Mohammad, K., & Jahanpour, A. (2018). Determinants of physicians' technology acceptance for mobile health services in healthcare settings. *Journal of Health Management & Informatics*, *5*(1), 9-15. Retrieved from http://jhmi.sums.ac.ir/index.php/JHMI/article/view/439/136

Sahdev, T., Medudula, M., & Sagar, M. (2014). An analysis of barriers for the adoption of cloud computing in education sector. *Management and Labour Studies*, *39*(3), 249-274. doi:10.1177/0258042X15572422

Samnani, A. K., & Singh, P. (2013). Exploring the fit perspective: An ethnographic approach. *Human Resource Management, 52*(1), 123-144. doi:10.1002/hrm.21516

Sandu, R., Gide, E., & Karim, S. (2017). The impact of innovative strategies to influence the adoption of cloud based service success in Indian small and medium enterprises (SMEs). *International Journal of Arts & Sciences, 10*(2), 389-399. Retrieved from http://www.universitypublications.net/ijas/1002/html/P7RS180.xml

Saswade, N., Bharadi, V., & Zanzane, Y. (2016). Virtual machine monitoring in cloud computing. *Procedia Computer Science, 79,* 135-142. doi:10.1016/j.procs.2016.03.018

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. doi:10.1057/jit.2014.25

Schoonenboom, J. (2014). Using an adapted, task-level technology acceptance model to explain why instructors in higher education intend to use some learning management system tools more than others. *Computers & Education, 71*, 247-256. doi:10.1016/j.compedu.2013.09.016

Scrutton, R., & Beames, S. (2015). Measuring the unmeasurable: Upholding rigor in quantitative studies of personal and social development in outdoor adventure education. *Journal of Experiential Education, 38*(1), 8-25. doi:10.1177/1053825913514730

Shakir, M., Abubakar, A., Yousoff, Y., Waseem, M., & Al-Emran, M. (2016). Model of security level classification for data in hybrid cloud computing. *Journal of Theoretical & Applied Information Technology, 94*(1), 133. Retrieved from http://www.jatit.org/volumes/Vol94No1/13Vol94No1.pdf

Shamala, P., Ahmad, R., Zolait, A. H., & bin Sahib, S. (2015). Collective information structure model for information security risk assessment (ISRA). *Journal of Systems and Information Technology, 17*(2), 193-219. doi:10.1108/JSIT-02-2015-0013

Sharafizad, J. (2016). Women business owners' adoption of information and communication technology. *Journal of Systems and Information Technology, 18*(4), 331-345. doi:10.1108/JSIT-07-2016-0048

Sharif, M. H., Troshani, I., & Davidson, R. (2015). Public sector adoption of social media. *Journal of Computer Information Systems, 55*(4), 53-61. doi:10.1080/08874417.2015.11645787

Sharma, S. K., Al-Badi, A. H., Govindaluri, S. M., & Al-Kharusi, M. H. (2016). Predicting motivators of cloud computing adoption: A developing country perspective. *Computers in Human Behavior, 62,* 61-69. doi:10.1016/j.chb.2016.03.073

Shiau, W., & Chau, P. Y. (2016). Understanding behavioral intention to use a cloud computing classroom: A multiple model comparison approach. *Information & Management, 53,* 355-365. doi:10.1016/j.im.2015.10.004

Shin, J., Jo, M., Lee, J., & Lee, D. (2014). Strategic management of cloud computing services: focusing on consumer adoption behavior. *IEEE Transactions on Engineering Management, 61*(3), 419-427. doi:10.1109/TEM.2013.2295829

Soni, M. (2015). End to end automation on cloud with build pipeline: The case for devops in insurance industry, continuous integration, continuous testing, and continuous delivery. *2015 IEEE International Conference on Cloud Computing in Emerging Markets (CCEM), 85*. doi:10.1109/CCEM.2015.29

Stallings, W., & Brown, L. (2014). *Computer security: Principles and practice* (3rd ed.). Upper Saddle River, NJ: Prentice Hall.

Stern, C., Jordan, Z., & McArthur, A. (2014). Developing the review question and inclusion criteria. *American Journal of Nursing*, *114*(4), 53-56. doi:10.1097/01.NAJ.0000445689.67800.86

Stieninger, M., Nedbal, D., Wetzlinger, W., Wagner, G., & Erskine, M. A. (2014). Impacts on the organizational adoption of cloud computing: A reconceptualization of influencing factors. *Procedia Technology*, *16*, 85-93. doi:10.1016/j.protcy.2014.10.071

Sugihara, T., Fujinami, T., Jones, R., Kadowaki, K., & Ando, M. (2015). Enhancing care homes with assistive video technology for distributed caregiving. *AI & Society, 30*(4), 509-518. doi:10.1007/s00146-014-0560-9

Sun, L., Dong, H., Hussain, F. K., Hussain, O. K., & Chang, E. (2014). Review: Cloud service selection: State-of-the-art and future research directions. *Journal of Network and Computer Applications*, *45*, 134-150. doi:10.1016/j.jnca.2014.07.019

Surendro, K., Supriana, A., & Supriana, I. (2016). Requirements engineering for cloud computing adaptive model. *Journal of Information and Communication Technology*, *15*(2), 1-17. Retrieved from http://jict.uum.edu.my/index.php/previous-issues/149-1

Svensson, L., & Doumas, K. (2013). Contextual and analytic qualities of research methods exemplified in research on teaching. *Qualitative Inquiry*, *19*, 441-450. doi:10.1177/1077800413482097

Taherdoost, H. (2018). Development of an adoption model to assess user acceptance of e-service technology: E-Service Technology Acceptance Model. *Behaviour & Information Technology, 37*(2), 173-197. doi:10.1080/0144929X.2018.1427793

Tang, C., & Liu, J. (2015). Selecting a trusted cloud service provider for your SaaS program. *Computers & Security*, *50*, 60-73. doi:10.1016/j.cose.2015.02.001

Tarmidi, M., Rasid, S. Z. A., Alrazi, B., & Roni, R. A. (2014). Cloud computing awareness and adoption among accounting practitioners in Malaysia. *Procedia-Social and Behavioral Sciences*, *164*, 569-574. doi:10.1016/j.sbspro.2014.11.147.

Thornham, H., & Cruz, E. G. (2018). Not just a number? NEETs, data and datalogical systems. *Information, Communication & Society, 21*(2), 306-321. doi:10.1080/1369118X.2017.1279204

Touray, A., Savolainen, T., Salminen, A., Sutinen, E., & Dai, Y. (2015). The role of trust in enhancing internet use in a high-risk society. *Journal of Systems and Information Technology, 17*(2), 141-166. doi:10.1108/JSIT-09-2014-0066

Tripathi, S. (2017). Understanding the determinants affecting the continuance intention to use cloud computing. *Journal of International Technology & Information Management, 26*(3), 124-152. Retrieved from http://scholarworks.lib.csusb.edu/jitim/vol26/iss3/

U.S. Department of Health & Human Services. (1979). *The Belmont Report*. Retrieved from http://www.hhs.gov/ohrp/humansubjects/guidance/belmont.html

Urquhart, L., Sailaja, N., & McAuley, D. (2018). Realising the right to data portability for the domestic Internet of things. *Personal & Ubiquitous Computing*, *22*(2), 317-332. doi:10.1007/s00779-017-1069-2

van Eyk, E., Toader, L., Talluri, S., Versluis, L., Uță, A., & Iosup, A. (2018). Serverless is more: From PaaS to present cloud computing. *Internet Computing, 22*(5), 8-17. doi:10.1109/MIC.2018.053681358

Van Horne, S., & Murniati, C. T. (2016). Faculty adoption of active learning classrooms. *Journal of Computing in Higher Education, 28*(1), 72-93. doi:10.1007/s12528-016-9107-z

Venkatesh, V., & Bala, H. (2008). Technology acceptance model 3 and a research agenda on interventions. Decision Sciences, 39(2), 273-315. doi:10.1111/j.1540-5915.2008.00192.x

Verma, S., Bhattacharyya, S. S., & Kumar, S. (2018). An extension of the technology acceptance model in the big data analytics system implementation environment. *Information Processing & Management, 54*(5), 791–806. doi:10.1016/j.ipm.2018.01.004

Virtual security appliances: The next generation security. (2015). *2015 International Conference on Communications, Management and Telecommunications (ComManTel), Communications, Management and Telecommunications (ComManTel), 2015 International Conference On*, 103. doi:10.1109/ComManTel.2015.7394269

Walsh, I. (2015). Using quantitative data in mixed-design grounded theory studies: An enhanced path to formal grounded theory in information systems. *European Journal of Information Systems, 24*(5), 531-557. doi:10.1057/ejis.2014.23

Wang, C., Wood, L. C., Abdul-Rahman, H., & Lee, Y. T. (2016). When traditional information technology project managers encounter the cloud: Opportunities and dilemmas in the transition to cloud services. *International Journal of Project Management, 34*(3), 371-388. doi:10.1016/j.ijproman.2015.11.006

Watson, C. (2015). Review of what is qualitative interviewing? And the problem-centred interview. *Qualitative Research, 15*(4), 540-542. doi:10.1177/1468794114535040

Wei, H., Ganjali, A., Beom Heyn, K., Sukwon, O., & Lie, D. (2015). The state of public infrastructure-as-a-service cloud security. *ACM Computing Surveys, 47*(4), 68:1-68:31. doi:10.1145/2767181

Wei, L., Zhu, H., Cao, Z., Dong, X., Jia, W., Chen, Y., & Vasilakos, A. (2014). Security and privacy for storage and computation in cloud computing. *Information Sciences, 258,* 371-386. doi:10.1016/j.ins.2013.04.028

Willcocks, L. P., Venters, W., & Whitley, E. A. (2013). Cloud sourcing and innovation: Slow train coming? *Strategic Outsourcing: An International Journal, 6*(2), 184-202. doi:10.1108/SO-04-2013-0004

Woiceshyn, J., & Daellenbach, U. (2018). Evaluating inductive vs deductive research in management studies. *Qualitative Research in Organizations & Management, 13*(2), 183. doi:10.1108/QROM-06-2017-1538

Wook, M. M., Yusof, Z., & Nazri, M. (2017). Educational data mining acceptance among undergraduate students. *Education & Information Technologies, 22*(3), 1195-1216. doi:10.1007/s10639-016-9485-x

Wu, H., & Feng-Kwei, W. (2015). A hybrid cloud model for cloud adoption by multinational enterprises. *Journal of Global Information Management, 23*(1), 1-23. doi:10.4018/jgim.2015010101

Yang, H. L., & Lin, S. L. (2015). User continuance intention to use cloud storage service. *Computers in Human Behavior, 52,* 219-232. doi:10.1016/j.chb.2015.05.057

Yang, Y., & Wang, X. (2019). Modeling the intention to use machine translation for student translators: An extension of Technology Acceptance Model. *Computers & Education, 133,* 116-126. doi:10.1016/j.compedu.2019.01.015

Ye, S., Liu, H., Leung, Y. W., & Chu, X. (2017). Reinsurance-emulated collaboration mechanism in cloud federation. *2017 IEEE 10th International Conference on Cloud Computing (CLOUD)*, Honolulu, CA, 727-732. doi:10.1109/CLOUD.2017.102

Yigitbasioglu, O. M. (2015). External auditors' perceptions of cloud computing adoption in Australia. *International Journal of Accounting Information Systems, 18*, 46-62. doi:10.1016/j.accinf.2015.09.001

Yilmaz, K. (2013). Comparison of quantitative and qualitative research traditions: Epistemological, theoretical, and methodological differences. *European Journal of Education, 48*(2), 311-325. doi:10.1111/ejed.12014

Yin, R. K. (2013). Validity and generalization in future case study evaluations. *Evaluation, 19*, 321-332. doi:10.1177/1356389013497081

Yin, R. K. (2014). *Case study research: Design and methods* (5th ed.). Thousand Oaks, CA: Sage Publications.

Young, D., Lopez, J., Rice, M., Ramsey, B., & McTasney, R. (2016). A framework for incorporating insurance in critical infrastructure cyber risk strategies. *International Journal of Critical Infrastructure Protection, 14*, 43-57. doi:10.1016/j.ijcip.2016.04.001

Zeqiri, A., Aliu, L., Kostanica, F., & Prenaj, B. (2017). An empirical investigation of cloud computing usage in education. *La Revue Des Sciences De Gestion, (285/286)*, 77-85. doi:10.3917/rsg.285.0077

Zissis, D., & Lekkas, D. (2012). Addressing cloud computing security issues. *Future Generation Computer Systems*, *28*(3), 583-592. doi:10.1016/j.future.2010.12.006

Appendix A: Interview Protocol

Interviewee (Title): _____

Interviewer: Nekerral Polk_____

Background:

_____ A: Demographics Questions

_____ B: Interview Questions

Other Topics Discussed: _____

_____

Documents Obtained: _____

_____

Post Interview Comments or Leads:

_____

Introductory Protocol

To facilitate our note-taking, I would like to audio record our conversations today. For your information, only researchers on the project will be privy to the recordings which will be eventually destroyed after they are transcribed. In addition, you must sign a form devised to meet our human subject requirements. Essentially, this document states that: (1) all information will be held confidential, (2) your participation is voluntary and you may stop at any time if you feel uncomfortable, and (3) we do not intend to inflict any harm. Thank you for your agreeing to participate.

I have planned this interview to last between 45 to 60 minutes. During this time, I will have several questions that I would like to cover. May I have your permission to start the recording and proceed with the interview.

Introduction

You have been selected to speak with me today because you have been identified as someone with the authority to impact decisions concerning strategies for adopting cloud computing services for your respective business unit. My research study will focus on strategies used by IT architects when adopting cloud computing services. The results of my study may provide other IT architects with valuable insight in to specific strategies to improve their cloud computing services implementations.

A. Demographics Questions

B. Interview Questions

Post Interview Comments and/or Observations:

Appendix B: Introductory Posting to Participants

Hello Mr. XXXXX,

My name is Nekerral Polk and I am a doctoral student at Walden University. I am at the point in my program where I have to conduct my research study to graduate. I would consider it an honor if you will participate in research study. I am performing a study on the adoption of cloud computing services with an insurance company. The purpose of this study is to explore strategies used by IT architects when deciding to adopt cloud computing services. This study is strictly a volunteer decision, and you may opt out whenever you decide. Participation in the study involves an interview to collect data. The interview will be audio recorded and later transcribed for the purpose of data analysis. I will only report on data that is confirmed and approved by you. I would like to thank you in advance and I can be reached at nekerral.polk@waldenu.edu.

Sincerely,

Nekerral Polk
Walden University
Doctoral Student

Appendix C: Confidentiality Agreement

Name of Signer: _____

During the course of my activity in collecting data for this research: I, Nekerral Polk will have access to information, which is confidential and should not be disclosed. I acknowledge that the information must remain confidential, and that improper disclosure of confidential information can be damaging to the participant.

By signing this Confidentiality Agreement, I acknowledge and agree that:

1. I will not disclose or discuss any confidential information with others, including friends or family.
2. I will not in any way divulge copy, release, sell, and loan, alter or destroy any confidential information except as properly authorized.
3. I will not discuss confidential information where others can overhear the conversation. I understand that it is not acceptable to discuss confidential information even if the participant's name is not used.
4. I will not make any unauthorized transmissions, inquiries, modification or purging of confidential information.
5. I agree that my obligations under this agreement will continue after termination of the job that I will perform.
6. I understand that violation of this agreement will have legal implications.

7. I will only access or use systems or devices I am officially authorized to access and I will not demonstrate the operation or function of systems or devices to unauthorized individuals.

By signing this document, I acknowledge that I have read the agreement and I agree to comply with all the terms and conditions stated above.

Signature: _____ Date: _____

Appendix D: Interview Questions

Demographic Questions

1. What is your role in the organization?
2. How long have you been in your current role?
3. How many years of experience do you have as an IT architect?
4. Do you have the authority to impact decisions concerning strategies for adopting cloud computing services for your respective business unit?

Interview Questions

1. What strategies have you used to adopt cloud computing services? How would you describe the usefulness of those strategies to the overall success of adopting cloud computing services?
2. What strategies did you use that were least effective in the adoption of cloud computing services? What made the strategies least effective? How easy were those strategies to implement?
3. What strategies did you use that were most effective in the adoption of cloud computing services? What made the strategies most effective? How easy were those strategies to implement?
4. What other strategies did you use that were effective in the adoption of cloud computing services? What made the other strategies effective? How easy were those strategies to implement?

5. In your experience, what issues prohibited cloud computing services adoption from being successful? Why did the issues prohibit the adoption from being successful?
6. What was your main concern in your strategy to adopt cloud computing services? Why did you have the concern? How easy was the concern to resolve?
7. What additional information is beneficial to add concerning IT strategies used to adopt cloud computing services?