BOURNEMOUTH UNIVERSITY

A DECISION FRAMEWORK TO MITIGATE VENDOR LOCK-IN RISKS IN CLOUD (SAAS) MIGRATION

JUSTICE NSIRIMOVU OPARA-MARTINS

BSc. MSc. FHEA (AMBCS)

Doctor of Philosophy

2017

A Decision Framework to Mitigate Vendor Lock-in Risks in Cloud (SaaS category) Migration

PhD Thesis

Justice Nsirimovu Opara-Martins BSc. MSc. FHEA (AMBCS)

A thesis submitted in partial fulfilment of the requirements for the degree of Doctor of Philosophy

May, 2017

Bournemouth University

Faculty of Science and Technology

Computing and Informatics Research Centre

1st Supervisor: Dr. Reza Sahandi Ph.D

2nd Supervisor: Dr. Feng Tian Ph.D

Copyright

Abstract

Cloud computing offers an innovative business model to enterprise IT services consumption and delivery. However, vendor lock-in is recognised as being a major barrier to the adoption of cloud computing, due to lack of standardisation. So far, current solutions and efforts tackling the vendor lock-in problem have been confined to/or are predominantly technology-oriented. Limited studies exist to analyse and highlight the complexity of vendor lock-in problem existing in the cloud environment. Consequently, customers are unaware of proprietary standards which inhibit interoperability and portability of applications when taking services from vendors. The complexity of the service offerings makes it imperative for businesses to use a clear and well understood decision process to procure, migrate and/or discontinue cloud services. To date, the expertise and technological solutions to simplify such transition and facilitate good decision making to avoid lock-in risks in the cloud are limited. Besides, little research investigations have been carried out to provide a cloud migration decision framework to assist enterprises to avoid lock-in risks when implementing cloud-based Software-as-a-Service (SaaS) solutions within existing environments. Such decision framework is important to reduce complexity and variations in implementation patterns on the cloud provider side, while at the same time minimizing potential switching cost for enterprises by resolving integration issues with existing IT infrastructures. Thus, the purpose of this thesis is to propose a decision framework to mitigate vendor lock-in risks in cloud (SaaS) migration. The framework follows a systematic literature review and analysis to present research findings containing factual and objective information, and business requirements for vendor-neutral interoperable cloud services, and/or when making architectural decisions for secure cloud migration and integration.

The underlying research procedure for this thesis investigation consists of a survey based on qualitative and quantitative approaches conducted to identify the main risk factors that give rise to cloud computing lock-in situations. Epistemologically, the research design consists of two distinct phases. In phase 1, qualitative data were collected using open-ended interviews with IT practitioners to explore the business-related issues of vendor lock-in affecting cloud adoption. Whereas the goal of phase 2 was to identify and evaluate the risks and opportunities of lock-in which affect stakeholders' decision-making about migrating to cloud-based solutions. In synthesis, the survey analysis and the framework proposed by this research (through its step-by-step approach), provides guidance on how enterprises can avoid being locked to individual cloud service providers. This reduces the risk of dependency on a cloud provider for service provision, especially if data portability, as the most fundamental aspect, is not enabled. Moreover, it also ensures appropriate pre-planning and due diligence so that the correct cloud service provider(s) with the most acceptable risks to vendor lock-in is chosen, and that the impact on the business is properly understood (upfront), managed (iteratively), and controlled (periodically). Each decision step within the framework prepares the way for the subsequent step, which supports a company to gather the correct information to make a right decision before proceeding to the next step. The reason for such an approach is to support an organisation with its planning and adaptation of the services to suit the business requirements and objectives. Furthermore, several strategies are proposed on how to avoid and mitigate lock-in risks when migrating to cloud computing. The strategies relate to contract, selection of vendors that support standardised formats and protocols regarding data structures and APIs, negotiating cloud service agreements (SLA) accordingly as well as developing awareness of commonalities and dependencies among cloud-based solutions. The implementation of proposed strategies and supporting framework has a great potential to reduce the risks of vendor lock-in.

Quotable from a notable:

"Indeed, one of my major complaints about the computer field is that whereas Newton could say, **"If I have seen a little farther than others, it is because I have stood on the shoulders of giants,"** I am forced to say, *"Today we stand on each other's feet."* Perhaps the central problem we face in all of computer science is how we are to get to the situation where we build on top of the work of others rather than redoing so much of it in a trivially different way. Science is supposed to be cumulative, not almost endless duplication of the same kind of things".

Richard Hamming 1968 Turning Award Lecture

Acknowledgements

First and foremost, I would like to thank God Almighty, whose many blessings have made me who I am today. In all honesty, it feels wonderful writing this page having just finished a decade at Universities in England, Great Britain (GB) in the United Kingdom. First it was at Southampton Solent University, then at the prestigious Bournemouth University (BU) for an MSc in Wireless and Mobile Networks, and now completing this PhD here at BU. I feel privilege to have accessed such a great academic community. The following document summarizes more than three years' worth of effort, frustration and achievement. However, I would like to express my great gratitude to everyone who has contributed during the process leading to my thesis. Here I would like to mention a few of them.

I am forever grateful to my supervisors; **Dr. Reza Sahandi** and **Dr. Feng Tian** for their encouragement, supervision, understanding, support, and above all their constructive and greatly appreciated invaluable feedbacks and critique throughout the research and thesis development process. I cannot express the extent to which their support and understanding allowed me to have successfully progressed to this point of the research journey. I wish to also thank Creg Handaz Nigeria Ltd. (co-sponsor) and Bournemouth University (BU) Studentship for match funding my PhD.

Throughout my time in the Faculty of Science and Technology, Computing and Informatics Research Centre, I have had the good fortune to work alongside many great minded, enthusiastic and fascinating academics and individuals. Special thanks to all the PGRs over the past three years with whom I have shared ideas, food, drinks and have also helped my time here at BU an enjoyable experience. Andrew Yearp, Adel Alkhalil, Alex Breen, Bruce Wen, Elizabeth Craig, Karim Abuowda and favourite colleague Navid Aslani, have provided the much-needed laughter, debate, politics and distraction – throughout the course of my studies. I would also like to thank Naomi Bailey for her impeccable administrative skills and support.

To my ex fiancée, Stephanie Onwordi, who stood tirelessly by me and supported every move towards my academic degree(s) and career pursuit, and have also been subjected to more rants about Cloud Computing and Information Technology jargon over the years than ought to be tolerable. Thank you so much baby, you are greatly appreciated. However, I'm not certain as to why the break-up prior to this PhD completion. Nonetheless, thank you very much for the time well spent.

I would also like to specially thank my family who have supported and encouraged me throughout my personal life and academic trajectory despite my shortcomings as an imperfect being. It should be known that without the continued emotional, spiritual and financial support provided by family, I may not have embarked on this journey. Therefore, special thanks go to my family (especially Mum), my awesome brothers (Reggie and Chizi) and my irreplaceable lovely-sister (Chisa) for their moral support, patience, prayers and love.

Finally, I wish to dedicate this PhD award to my beloved father (*HRH Chief Christian Owhonda Opara-Martins*) who passed away, on the 13th of January 2013, less than a week from enrolling as a PhD scholar. This PhD thesis is dedicated to you, **Dad!** for believing and instilling in me the drive for continuous success, love for knowledge, humility and above all the eternal fear of God. To Dad, I love you now, forever, and always. To my late big-brother (*Leslie Ogechi "Chimenem" Opara-Martins*), I did this for us, love and miss you now, always and forever big-bro.

Thank you very much.

Contents

Declaration

Author's Declaration

I, Justice Nsirimovu Opara-Martins, hereby certify that this thesis, which is approximately 80,000 words in length, has been written by me, that it is the record of work carried out by me and that it has not been submitted in any previous application for a higher degree, nor been accepted in candidature for any other award.

I was admitted as a researcher in Cloud Computing and as a candidate for the degree of Doctor of Philosophy in January 2013 to the Faculty of Science and Technology, in Bournemouth University between 2013 and 2017.

I declare that while registered as a candidate for the research degree, I have not been a registered candidate or enrolled student for another award of the university, other academic or professional institution.

Signature of Candidate: Justice Nsirimovu Opara-Martins BSc. MSc. FHEA (AMBCS)

(Sign here) **……**

Date: May 2017

Type of Award: Doctor of Philosophy

School / Department: Faculty of Science and Technology

Centre: Computing and Informatics Research Centre

List of Figures

List of Tables

Publications

The research study detailed in this thesis has yielded several internationally recognized peer-reviewed journals, book chapters, and conference publications in the areas of cloud computing, virtualization, information and communication technologies (ICT), and distributed computing systems. These include:

Journal Papers

1. Opara-Martins, J., Sahandi, R. and Tian, F., 2017, August. "A Holistic Decision Framework to Avoid Vendor Lock-in for Cloud SaaS Migration." In *Computer and Information Science*, *10*(3), p.29. http://doi.org/10.5539/cis.v10n3p29

2. Opara-Martins, J., Sahandi, R. and Tian, F., 2017, March. "Six-Step Decision Framework to Avoid Vendor Lock-in Risks in Cloud Migration." In: Journal of Cloud Computing: Advances, Systems and Applications. SpringerOpen doi: (pending)

3. Opara-Martins J., Sahandi, R. and Tian, F., 2017, June. "Cloud SaaS Migration: Decision Framework to Avoid Vendor Lock-in Risks." In: *Journal of Computer Information Systems* doi: (pending)

4. Opara-Martins, J., Sahandi, R. and Tian, F., 2017, June. "A Systematic Review Protocol for Cloud Migration approaches to Avoid Vendor Lock-in." In: *Computer and Information Science Journal*. doi:

5. Opara-Martins, J., Sahandi, R. and Tian, F., 2016, April. "Critical analysis of vendor lock-in and its impact on cloud computing migration: a business perspective." In: *Journal of Cloud Computing: Advances, Systems and Applications* (2016) 5:4. SpringerOpen. doi: 10.1186/s13677-016-0054-z

6. Sahandi, R., Alkhalil, A. and Opara-Martins, J., 2013, March. "Cloud computing from SMEs perspective: a survey based investigation." In: *Journal of Information Technology Management*, *24*(1), pp.1-12. ISSN #1042-1319

Conference Proceedings

7. Opara-Martins, J., Sahandi, R. and Tian, F., 2015, November. "A Business Analysis of Cloud Computing: Data Security and Contract Lock-In Issues." In: *10th International Conference on P2P, Parallel, Grid, Cloud and Internet Computing (3PGCIC)*, Krakow, *Poland*, 2015, pp. 665-670.IEEE doi: 10.1109/3PGCIC.2015.62

8. Opara-Martins, J., Sahandi, R. and Tian, F., 2014, November. “Critical review of vendor lock-in and its impact on adoption of cloud computing.” In: *Information Society (i-Society), 2014 International Conference, (i-Society 2014),* London, UK, pp. 92-97. IEEE. doi: 10.1109/i-Society.2014.7009018

Book Chapters

9. Opara-Martins, J., Sahandi, R. and Tian, F., 2015, October. "Implications of Integration and Interoperability for Enterprise Cloud-based Applications." In: *6th International Conference on Cloud Computing (CloudComp), Daejeon, South Korea, 2015, pp. 213-223.* SpringerVerlag in the Lecture Notes of ICST (LNICST). doi: 10.1007/978-3-319-38904-2_22

10. Sahandi, R., Alkhalil, A. and Opara-Martins, J., 2013, October. “SMEs’ Perception of Cloud Computing: Potential and Security.” In *Collaborative networks in the internet of services: 13th IFIP WG 5.5 working conference on virtual enterprises, PRO-VE 2012,* Bournemouth, UK, October 2012: proceedings, pp.186-195. Springer Berlin Heidelberg. doi: 10.1007/978-3-642-32775-9_19

Chapter one

1. Introduction

Cloud computing as a new information technology (IT) paradigm, offers unprecedented scalability to an organisation's business processes and business operations (Sitaram and Manjunath, 2012). The cloud technology allows organizations to expand or reduce their computing facilities very quickly. This concept is attracting public and private companies, as well as small to medium-sized enterprises (SMEs), who consider cloud computing model an opportunistic business strategy to remain competitive and to meet business needs (Armbrust et al. 2010; Buyya et al. 2009; Andrikopoulos et al. 2013). Larger enterprises are exploiting the benefits of this platform by taking business continuity into account, while SMEs to the contrary are enhancing their ability to meet computing resource demands, while eschewing consequential investment in over provisioned infrastructure, maintenance, training etc. (Jamshidi et al. 2013). The supply of information technology (IT) in the cloud has been enabled both by the evolution of sophisticated data centres (e.g. software defined network or SDDC) and widespread access to improved network bandwidth (BCS, 2012). In essence, these technical advances mean that traditional IT services such as data storage, servers, networks etc. are hosted on physical machines across a wide range of locations. But from the business (i.e. consumer and end-user) perspective, they simply are virtualised resources residing in the 'cloud'. In other words, the term 'cloud' is simply a new way in which business is done and IT is provided. Broadly speaking, cloud computing is a natural evolution of business model in IT services consumption and delivery. While it is important to disambiguate the term for practical reasons, the rest of this paper embodies and assumes such definition. A unique business advantage of this model of IT service provision is the ubiquitous access it provides to customers to improve their ability to access applications and data from remote locations (location independence) and multiple devices (device independence). Delivered in this manner, the functionality can either be at the infrastructure level, platform or at the application level.

The concept of cloud computing is to offer an opportunistic business strategy to enterprises (small or large), to remain competitive and meet business needs (Andrikopoulos et al., 2013; Armbrust et al., 2009; Buyya et al., 2009). Whilst this concept seems like an attractive proposition for both public and private companies, several challenges remain inadequately addressed. A recent survey conducted by Sahandi et al. (2013) reported security and vendor lock-in as major barriers to cloud adoption across the United Kingdom (UK) market. The European Network and Information Security Agency (ENISA) and European Commission (EC) have recognized the vendor lock-in problem as a one of the greatest obstacles to enterprise cloud adoption (Loutas et al, 2011). Per (Toivonen, 2013), market demand and the ability to attract more customers are creating more pressure on cloud

providers to support interoperability – a direct benefit of avoiding vendor lock-in. Vendor lock-in problem in cloud computing is characterized by expensive and time-consuming migration of application and data to alternative providers (Wang, 2013). Cloud software vendors lock-in customers in several ways: (1) by designing a system incompatible with software developed by other vendors; (2) by using proprietary standards or closed architectures that lack interoperability with other applications; (3) by licensing the software under exclusive conditions (Miranda, 2012). Vendor lock-in deters organizations adopting cloud technology. It is a challenging issue that requires substantial efforts to overcome the existing barriers it erects for enterprises migrating to cloud-based solutions (Toivonen, 2013).

The reviews of existing literature (de Oliveira et al. 2017; Garcia et al. 2016; Di Martino et al. 2015; Stravoskoufos et al. 2014; Toosi et al. 2013; Di Martino et al. 2014; Satzger et al. 2013; Binz et al. 2014; Binz et al. 2012; Petcu et al. 2013; Adagna et al. 2012; Kratzke, 2014), have shown that previous studies have focused more on interoperability and portability issues of cloud computing when lock-in is discussed. Amongst many problems being discussed are: the lack of standard interfaces and open APIs (Open Group, 2016), the lack of open standards for VM format (Ferry et al. 2014) and service deployment interfaces (Silva et al. 2013; Opara-Martins et al. 2014), as well as lack of open formats for data interchange (Fowley et al. 2017; Opara-Martins et al. 2016). These issues result in difficulties in integration between services obtained from different cloud providers as well as between cloud resources and internal legacy systems (Edmonds et al. 2012). Consequently, this renders the interoperability and portability of data and application services difficult. The emergent difficulty is a direct result of the current differences between individual cloud vendors' offerings based on non-compatible underlying technologies and proprietary standards. Cloud providers often propose their own solutions and proprietary interfaces for access to resources and services. This heterogeneity of cloud provider solutions (i.e. hardware and software) and service interfaces is a crucial problem since most of the current resources bind the customer to stick with one cloud technology due to high cost in porting the applications and data to a different provider's interface. The heterogeneity in cloud computing is simply the existence of differentiated hardware, architectures, infrastructure, and technology used by cloud providers. Many cloud vendors provide services based on custom-built policies, infrastructure, platforms, and APIs that make the overall cloud landscape heterogeneous. Such variations cause interoperability, portability, and integration very challenging. Following the principle that compatible interfaces are important in a cloud environment, two implementations of the same cloud service may store and process data very differently. This may well also involve storing derived and implementation specific data differently (Opara-Martins et al. 2016; Kalloniatis et al. 2014). Without proper definitions for import and export formats, a set of data from one service implementation will probably be meaningless when imported into another cloud service. For example, a cloud service may be accessed and used by a wide variety of clients, including mobile,

desktops and even tablet PCs. However, the information created and consumed by those services can still be limited to a single vendor if a proprietary data format is used. Further, this can create a degree of instability and data incompatibility issue as interfaces to the functionality may be proprietary, and thus any solution that is built to leverage the functionality provided cannot be easily migrated to a competitive cloud service offering (Nelson-Smith, 2011). So, while customers might be able to access and use the services from a variety of clients, the ability to move seamlessly from one vendor to another may be difficult because of other dependencies such as different data formats. Clearly, this problem has an impact on interoperability and data portability between clouds.

At the core of all these problems, we can identify concerns about consumers' demand to migrate data to and from different clouds (data portability), and interoperability between clouds. Research has already addressed movability and migration on a functional level (Fowley et al. 2017; Wettinger et al. 2014a; Kalloniatis et al. 2014; Rafique et al. 2014). However, migration is currently far from being trivial. The two main reasons are the lack of world-wide adopted standards or interfaces to leverage the dynamic landscape of cloud related offers (Wettinger et al. 2014b), and absence of standards for defining parameters for cloud applications and their management. Without an appropriate standardized format, ensuring interoperability, portability, compliance, trust, and security is difficult (Hummer et al. 2013). Standards continue to rapidly evolve in step with technology. Hence, standards may be at different stages of maturity and levels of acceptance. But, unless the standards are well-accepted and widely used, such standards remain a questionable solution [8]. In other words, a partially adopted standard would represent a poor solution. Essentially, this explicit lack of standards to support portability and interoperability among cloud providers stifles the market competition and locks customers to a single cloud provider (Toosi et al. 2013). To expatiate further, potential difficulties (by primarily technological means) in achieving interoperability and portability lead to lock-in – resulting in customer dependency on the services of a single cloud computing provider (Opara-Martins et al. 2014). From a legal stance, the dependency can be aggravated by the abusive conduct of a cloud computing provider within the meaning of Article 102 TFEU (Treaty on the Functioning of the European Union) (Vanberg et al. 2017; Opara-Martins et al. 2016), where other providers are excluded from competing from the customers of the initial cloud provider. In such situations, limitations to interoperability and portability could be an abuse by a dominant provider using this practice as a technical means to stifle (i.e. monopolize) competition. Such practices distort competition and harm consumers by depriving them of better prices, greater choices and innovation. Hence, the competition law has the role of ensuring competition is maintained and enforced in the market by regulating anti-competitive conduct by cloud providers. To this end, it can be concluded that cloud interoperability (and data portability) constraints are potential results of anti-competitive environment created by offering services with proprietary standards.

1.1 Background

As organisations interact with service providers in the current cloud marketplace they encounter significant lock-in challenges to deploying, migrating, and interconnecting cloud services in a manner considered satisfactory. To date, the expertise and technological solutions to simplify such transition and facilitate good decision making are limited. Consequently, most customers are unaware of proprietary standards which inhibit interoperability and portability of applications when taking services from vendors. Interoperability and portability are essential qualities that affect the cloud under different perspectives (Di Martino, 2015; Petcu, 2011; Opara-Martins et al. 2014; Open Group, 2016), due to the risk of vendor lock-in. In effect, while many studies cite vendor lock-in as a major barrier to cloud computing adoption (Petcu and Vasilakos, 2014; Buyya et al. 2009; Liu and Ye, 2008; Bradshaw et al. 2012; Badger et al. 2011; Ahronovitz, 2010), yet due to its complexity, a lack of clarity still pervades (Opara-Martins et al. 2016). Without a clear insight into how such complex decision is made to avoid lock-in, it is difficult to identify gaps where further research is beneficial for business adopters. Current solutions and efforts tackling the vendor lock-in problem are predominantly technology-oriented. Such approach is compromised by ignoring organisations' awareness and perception of the lock-in problem. For example, how is cloud lock-in experienced or understood from the business stance? Limited in-depth studies exist to investigate the complexity of cloud lock-in problem within enterprise organisations. Likewise, the customers, who are willing to choose the cloud services without being strictly bound to a specific solution, are mostly neglected. Moreover, limited research work has been carried out to provide a cloud migration framework to assist enterprises avoid vendor lock-in risks when implementing cloud-based Software-as-a-Service (SaaS) solutions within exiting environments. Such framework is important to reduce complexity and variations in implementation patterns on the cloud provider side, while at the same time minimizing potential switching cost for enterprises by resolving integration issues with existing IT infrastructures.

Advances in cloud computing research have in recent years resulted in a growing interest for migration towards the cloud. But due to concerns about the risks of vendor lock-in, as noted by (Leymann et al. 2011), organisations would particularly welcome standards that address application migration (e.g. Open Virtualization Format (OVF)) and data migration (e.g. Amazon S3 API) because such standards mitigate lock-in concerns. Various standardisation solutions from different industry bodies have been developed for increasing interoperability and portability within diverse cloud computing services (Shan et al. 2012; Toivonen, 2013). However, initiatives by multiple standard bodies, researchers, and consortiums could indirectly lead to the possibility of multiple standards emerging with possible lack of consensus, thereby deteriorating the lock-in problem even further. The main problem is attributed to the fact that currently each provider develops its own specific technology solutions, remote APIs, and some even create new programming languages (Wang, 2013).

Because of this, cloud users become dependent (i.e. locked-in) on a certain vendor's services and are unable to switch to different vendor–due to technical incompatibilities–without undertaking substantial switching costs (Stravoskoufos, 2014). To further complicate issues, for instance switching between alternative vendors, of essentially the same product, without paying substantial switching cost is not possible as argued by (Zhu and Zhou, 2011). In other words, the substantial cost associated with switching between incompatible cloud software systems and vendors can force a customer to use the same products and services. Thus, consumer choices of cloud-based services and solutions may exhibit path dependency: decisions by earlier adopters can be expected to have some effect on the decisions of later adopters.

1.2 Research Question(s)

The underpinning research question explored within this thesis can be stated as follows:

> *How can enterprises achieve the portability and interoperability of SaaS (applications and data) services across cloud provider's technology platforms and storage systems while expanding functionality for migration via hybrid cloud techniques to mitigate the lock-in problem?*

Despite these legitimate concerns and technical complexity of vendor lock-in, this PhD study aims to answer the following two questions of interest to business adopters of cloud services and solutions:

1) How to avoid being locked-in to a single cloud service provider?

2) How easy is it to deploy existing cloud SaaS artefacts (e.g. data, metadata, and application components) on another service provider's technology platform without modification to the artefacts – which would reduce the financial benefit of the migration?

The former applies more to companies who have migrated or are looking to adopt more cloud solutions, whereas the latter is closely related to companies considering moving core systems into the cloud environment. Giving answers to these questions is deceptively easy and straightforward, but the reality is different. Presently, for many companies, there is a large amount of sensitive data and IT assets in-house which can deter them to migrate to the cloud due to risks of vendor lock-in, security and privacy issues. For these reasons, it becomes not only critical to consider security and privacy concerns but also related issues such as integration, portability, and interoperability between the software on premise and in the cloud (Lewis, 2015), should be taking aboard. Therefore, organisations must be aware of appropriate standards and protocols used by cloud providers to support data/application movability. Moreover, the ease of moving data across (i.e. portability) cloud providers' platform mandates data to be in a compatible format (Petcu, 2011), and includes the need to securely delete the old storage (Hogan et al. 2011). In other words, the ability to move

data/application about is of crucial importance, as much as the effort involved in moving – inability to achieve this portends large as a management issue for cloud computing. To further complicate matters, maintaining compliance with governmental regulations and industry requirements adds another layer of considerations to the management of data. Whether organisations can easily shift their data/application about seamlessly, remains one of the biggest issues facing cloud adoption across diverse industries. Addressing these questions will support enterprises and decision makers with their strategies for migration, and when considering designing and develop interoperable applications to avoid lock-in and integrate seamlessly into other cloud and on-premise systems.

1.3 Aim and Objectives

The main aim of this research is to propose a decision framework to avoid vendor lock-in risks in cloud migration.

Research Objectives:

O.1. Explore views of professional practitioners on issues associated with cloud vendor lock-in.

O.2. Identify, analyse and explore the technical, legal, and business issues associated with cloud vendor lock-in.

O.3. Identify policy and industry recommendations that could potentially steer the development of a vendor-neutral cloud marketplace.

- Identify standards that support interoperability between different cloud providers network.
- Identify standards that facilitate the portability of data from one vendor to another.
- Examine limitations in existing cloud service contracts and Service Level Agreement (SLA) that fail to tackle the risks of vendor lock-in, and review their implications for businesses adopting cloud computing

O.4. Review typical cloud providers' standard contract terms of services and SLAs as an attempt to identify the contractual issues which need to be addressed in order to enable the cloud-to-cloud migration or on-premise-to-cloud-based SaaS application modernisation.

O.5. Propose a novel holistic decision framework to avoid vendor lock-in risks in cloud (SaaS category) migration.

O.6. Evaluate the proposed framework based on expert opinions and practitioners' review

1.4 Contributions

This PhD research work makes several contributions to academic knowledge and practice. The principal contribution was to meet the main aim of this research study by developing a cloud migration decision framework to avoid vendor lock-in risks, and in supporting enterprise cloud adoption decision making process. An important secondary contribution, however, is that the overall research work added substantially to the growing body of knowledge on cloud computing adoption and migration by examining the factors that influence cloud adoption and/or deter cloud migration decisions within organisations that are transforming their businesses using cloud computing technologies.

In summary, this thesis and the PhD research work it is based on make the following contributions (abbreviated as **C**) to knowledge:

C1. A critical review of vendor lock-in and its impact on adoption and migration to cloud computing.

C2. Clarification of the vendor lock-in phenomenon within the cloud computing environment, and a subsequent analysis of the main risk factors that contribute to cloud lock-in situations.

C3. A systematic review study of issues associated with migration to the cloud and vendor lock-in problem. This also incorporates a critical appraisal of existing decision frameworks, models and processes which support cloud computing adoption and migration in enterprises.

C4. The formulation of a cloud computing vendor lock-in taxonomy which have been organised into hierarchical categories of perspectives. Note; the proposed taxonomy partitions the associated lock-in challenges to address into three viewpoints; business, technical, and legal. Each of the viewpoints can be used as problem analysis technique as well as solution space of the relevant issues of the lock-in problem domain.

C5. The manifestation and implications of how integration and interoperability concerns affect enterprise cloud-based application migration and adoption.

C6. A critical business analysis of cloud computing from a data security and contract lock-in perspectives.

C7. A novel decision framework, with supporting strategies to avoid vendor lock-in risks in cloud computing SaaS migration at the strategic, tactical and operational levels.

1.5 Organisation of Thesis

This thesis has been divided into seven (7) chapters. The content of the chapters is summarised as follows:

Chapter one: discusses the background and the motivation of the research; based on the discussion of the background literature, the primary research aim, research questions and objectives are developed. The research contributions (abbreviated as **C**) and an outline of the research is given. Overall, this chapter aims to justify and clarify the research problem that is being investigated in this PhD thesis.

Chapter two: provides a comprehensive background and critical appraisal of cloud computing literature, focusing on evolution of computing systems, cloud computing characteristics and reference architecture (CCRA), cloud computing application architectures, heterogeneity roots in the cloud environment and cloud computing migration approaches. The discussion of issues related to interoperability, portability, and standards are presented and the chapter also deliberates on the implications of integration and interoperability for enterprise applications, as well as approaches enabling portability and interoperability to support cloud computing adoption. This chapter concludes by highlighting the main business benefits and challenges faced by organisations adopting and migrating to cloud-based services. Note, this chapter may seem comprehensive in context, however its aim is meant to explain and justify the research objectives raised in chapter one.

Chapter three: provides the theoretical underpinning for this research by discussing the vendor lock-in problem faced by enterprises in the context of cloud computing environments. Based on the complexity of cloud lock-in risks hindering adoption and migration decisions in the enterprise, this chapter identify and categorises the main risk factors that intensify and/or trigger cloud SaaS lock-in situations. The identification of the main SaaS lock-in risks resulted from a systematic literature review (SLR) conducted to identify challenges associated with switching/changing between cloud SaaS vendors. Based on the critical analysis of this factors, taxonomy of vendor lock-in perspectives have been defined and discussed comprehensively in this chapter which are the foundations of the cloud migration decision framework and the supporting strategies.

Chapter four: presents the detailed research methodology used in this study to fulfil the overarching research aim and questions posed in chapter one. The implementation of the research design (based on qualitative and quantitative approaches) and the subsequent analysis of the empirical data are discussed in this chapter. Implications or observations drawn from the key findings are also discussed herein.

Chapter five: presents the development of the proposed six-step decision framework to avoid vendor lock-in risks in cloud computing migration. This chapter comprehensively discusses the 6-step decision framework that enables an enterprise to assess its current IT landscape for potential SaaS

replacement, and provides effective prescriptive (i.e. tactical and operational) strategies to mitigate vendor lock-in risks in cloud (SaaS) migration. The decision framework follows research findings and addresses the core requirements for choosing vendor-neutral interoperable and portable cloud services without the fear of vendor lock-in, and architectural decisions for secure SaaS migration. Therefore, the results of this research can help IT managers have a safe and effective migration to cloud computing SaaS environment.

This chapter also elaborates on the proposed 6-step decision framework. The decision framework through its step-by-step approach provides guidance on how to avoid being locked into individual cloud service providers. This reduces the risk of dependency on a cloud provider for service provision, especially if data portability, as the most fundamental aspect, is not enabled. Each decision step within the framework prepares the way for the subsequent step, which supports a company to gather the right information to make a right decision before proceeding to the next step. The reason for such an approach is to support an organisation with its planning and adaptation of the services to suit the business requirements and objectives. Furthermore, this chapter also discusses the process of validation and evaluation of the proposed decision framework based on the analysis of the views of cloud and industry practitioners, IT managers and academia.

Chapter six: encapsulates the outcomes of this research and draws conclusion for this thesis by summarising the novel contributions made. This chapter concludes by highlighting the implications of this research and further identifies and describes areas for future work.

1.6 Chapter Summary

Cloud computing adoption and migration is a topical issue, and there is significant interest from academia and industry in using cloud-based services and solutions. Since, as academics, we are uniquely positioned to offer unbiased advice and expertise to enterprises that are interested in consuming or using new technologies such as cloud computing. Therefore, the work presented herein is rooted in academic research and fills a gap in the current cloud computing literature, also provides a vendor-neutral expertise and proposal framework for companies that are interested in deploying or migrating cloud-based SaaS environments. This research study is concerned with supporting the decision-making process to avoid vendor lock-in risks for cloud-to-cloud migration and/or migrating/replacing on-premise IT systems with cloud-based (SaaS) alternatives. This chapter provided an introduction to the concept of cloud computing vendor lock-in phenomenon, the business needs (or requirements) for organisations to avoid the lock-in problem, overarching research aim and objectives, thesis structure and finally, the novel contributions made thus far by this research work.

Chapter Two

2. Literature Review

2.1 Introduction

This chapter discusses the background and theory to the topics which are covered in this thesis report. The background of cloud computing, including the evolution of computing systems and the theory of lock-in is provided in this chapter. A concise analysis of issues associated with vendor lock-in, integration and interoperability implications, and its impact on enterprise migration is presented. As the scope of this research is within the field of enterprise cloud migration, the theoretical concepts behind this shift are discussed. To justify the novelty of this research, a review of existing approaches and standards to tackle lock-in challenges in cloud environment, and methodologies for enabling interoperability and portability is conducted. Key legal issues and security concerns are provided herein.

2.2 Evolution of Computing Systems

To fully comprehend how cloud computing has evolved it is important to understand the evolution of computing from a historical perspective, focusing primarily on those advances that led to the development of cloud computing, such as the transition from mainframe to desktops, laptops, mobile devices and on to the cloud (Rittinghouse & Ransome, 2010). The idea of providing a centralised computing service dates to the 1960s, when computing services where provided over a network using a mainframe time-sharing technology. During this period, the mainframe time-sharing mechanism effectively utilised computing resources, and provided acceptable performance to users; however, mainframes were difficult to scale and provision up-front because of high hardware costs.

In 1961, the Internet pioneer John McCarthy predicted that "someday computation may be organised as a public utility" and thus far, there has been a paradigm shift in the geography of computation. Later in the sixties, the idea of an intergalactic computer network was introduced by JCR Licklider who was liable for the development of Advanced Research Projects Agency Network (ARPANET) in 1969. According to (Mohammed, 2009), Lickliders vision for ARPANET was to create a computer network with the capability to interconnect everyone on the globe with access to numerous programs and data at any site, virtually from any location. This discussion is further substantiated by Margaret Lewis in a report published by (Hoover & Martin, 2008), adding that "the vision of ARPANET sounds a lot like what is being referred to as cloud computing today, – often in the IT industry when people talk about plug into IT cloud, they normally have something simple in mind; i.e. browser access to an application hosted on the web". Cloud computing is certainly that but there is also much to it. Cloud computing is a natural development to meet needs that have been evident for more than forty years (Sarna, 2011). Virtualization is the key technology that enables

cloud computing. In effect, remote hosting has developed from simply renting infrastructure to providing and maintaining standardized virtual servers that can be scaled up and down as demand fluctuates. Thus, the computing world is rapidly transforming towards developing software for millions to consume as a service, rather than rely on their individual computers (Carlson, 2011). Cloud computing indeed evolved out of Grid computing and relies on Grid computing as its backbone and infrastructure support. The evolution has been a result of a shift in focus from an infrastructure (that delivers storage and compute resources such is the case in Grids) to one that is economy based aiming to deliver more abstract resources and services (such is the case in clouds) (Foster et al. 2008).

Generally, it is difficult to tell whether a service is genuinely a cloud computing service offering or unambiguously a pre-existing offering that has the cloud label imposed on it by vendors, for example hosted service, on-demand computing, grid computing, utility computing, Software-as-a-Service (SaaS), Application Service Provider (ASP) etc. Service providers are expanding their available offerings to include the entire traditional IT stack, from hardware and platforms to application components, software services, and whole applications, as shown in **Figure 2.1**. Many vendors offer managed infrastructure and platforms as a service, but until there is a universally accepted standard between IT service providers of many types and consumers, vendors will continue to fight for competitive advantage. Independent software vendors (ISVs) and well as enterprise architects and developers are building robust, multitenant software-as-a-service applications to run efficiently on these platforms, and usage is anticipated to explode dependent on the emergence of widely used standards.

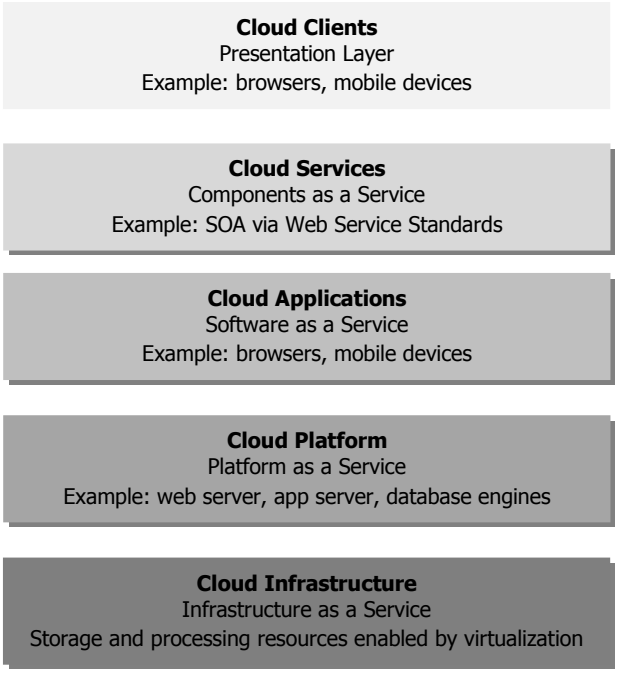


Figure 2.1- Cloud Computing Represented as a Stack of Service Offering (Adapted and Modified from [Johnston, 2008])

Cloud Computing and Distributed Systems

According to (Mascato et al., 2011), cloud computing is a model for distributed systems. A distributed system consists of a collection of autonomous computers, connected through a network and distribution middleware, which enables computers to coordinate their activities and to share the resources of the system, so that users perceive the system as a single, integrated computing facility (Emmerisch, 1997). While the concept of cloud computing addresses the next evolutionary step of distributed computing, its goal is to make use of distributed resources in order to achieve higher throughput to tackle large scale computation problems (Choi and Lumb, 2009). However, cloud computing differentiates itself from other distributed computing paradigms through its apparent infinite elasticity. Elasticity in this context is understood as the ability to on-demand scale-up and down the number of cloud resources allocated for an application (Petcu et al. 2012). For example, the adoption of clouds in enterprise is hindered by the fact that legacy codes need to be re-written in order to take advantage of elasticity. Besides distributed computing systems, cloud computing also draws from other pre-existing technologies such as virtualization, service oriented architecture (SOA), grid computing, or utility computing (Hwang, 2008; Milojicic, 2008; Weiss, 2007). The variety of technologies and architectures used in cloud computing makes the overall picture confusing due to the blurred boundaries among them (Hwang, 2008). Moreover, the increase in the number of service providers and IT vendors, nowadays, entering the cloud market, further hardens the analysis of the distinguishing features of this technology (Milojicic, 2008). To further complicate this situation, vendors provide different cloud services at different levels usually providing their own proprietary interfaces to users and Application Programming Interfaces (APIs) to developers, to leverage the dynamic landscape of cloud-related offers. This results in several problems for end-users that perform different operations for requesting cloud services provided by different vendors, using different interfaces, languages and APIs. Further, it also makes the global agreement of on an acceptable solution harder to achieve (Petcu et al. 2012).

Cloud computing has the potential to address the programmability of resources in general, either infrastructure or software resources. Current cloud computing infrastructure typically assumes a homogeneous collection of commodity hardware, with details about hardware variation intentionally hidden from users (Crago et al. 2011). Providers such as Amazon and Rackspace, as an example, provide users with access to a homogeneous set of commodity hardware through virtualization technology with little or no control of locality (except often by geographic region). Cloud technologies bring applications and infrastructure services mobility and (physical/hardware) platform independency to the existing distributed computing and networking applications. The provisioned cloud based infrastructure services may involve multi-provider and multi-domain resources, including integration with the legacy services and infrastructures. The cloud service provider often utilizes

virtualization technologies to separate application services from infrastructure in order to offer more efficient services to cloud service consumer, and optimize resource utilization. However, a complex aspect for service management is the semantic heterogeneity among different cloud service provider's policies, since they may have inconsistent approaches for implementing security mechanisms. This inconsistency can breed application and data fragmentation issues in the cloud, thus making it challenge to port data and application to varied cloud service providers. Moreover, as a result of this heterogeneity, deploying applications to a cloud and managing them needs to be done using vendor specific methods and tools. This level of lock-in or dependency (on service provider tools) is seen as a major hurdle in adopting cloud technologies to the enterprise. The main aspect of the lock-in problem affecting enterprise decisions spans across the lack of world-wide adopted standards, low level of portability and interoperability of applications and data services based in the cloud (refer to *Section 2.9*). Though the heterogeneity of cloud approaches among cloud service providers can encourage innovation and some level of adoption, it creates confusions in the marketplace for cloud service consumers with the risk of them creating cloud silos that are non-interoperable (i.e. cannot federate). To minimize the impact and occurrence of this risk, we stimulate our discussion by describing heterogeneity roots in the cloud ecosystem (*cf Section 2.7*).

Given that distributed systems and their delivery are at the core of cloud computing, all cloud computing related activities (or parties) can be categorised into three main groups: activities that use cloud services (i.e. cloud service customer), activities that provide cloud services (i.e. cloud service provider) and activities that support cloud services (i.e. cloud service partner). Parties in cloud computing system are its stakeholders. A party can play more than one role at any given time and can engage in a specific subset of activities of that role. These different activities could be likened to represent and/or describe some of the common roles and sub-roles associated with cloud computing. A cloud activity in this context is defined as a specified pursuit or set of tasks. Detailed descriptions of the cloud computing roles and sub-roles, and their relationship are presented in *Section 2.4.3*.

2.3 Cloud Computing Fundamentals

Cloud computing has become one of the most frequently cited and infrequently understood technology term pitched to IT buyers and analysts, enterprises, SMEs and the public at large as noted by (Juniper Media, 2009). While there may be confusion about the right definition of cloud computing, it should be underlined for the gullible readers that cloud computing is not a technology revolution, but rather a process and business revolution on how we use these technologies that enable cloud computing as it exists today. Typical example of these technologies may include: SaaS, Representational State Transfer (REST), Synchronous JavaScript and XML (SJAX), Service-Oriented Architectures (SOA), on-demand computing, Virtualization etc. At its nascent state, cloud computing lacks a consensus definition. There have been different proposing views by policy makers on its

definition. A report by Spinola (2009), confirmed that there were at least 22 different cloud computing definitions in use. But the state-of-the-art working definition of the cloud is designated to the National Institute of Standards and Technology (NIST) and it has been absorbed into this thesis.

According to NIST, cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction (Mell and Grance, 2011). This cloud model is composed of five essential characteristics, three service models, and four deployment models (i.e. cloud types) that are represented as layers in the cloud technology stack (see Figure 3): ranging from the cloud infrastructure (Infrastructure as a Service or IaaS); cloud application platform (Platform as a Service or PaaS); and cloud application (Software as a Service or SaaS) (Marks and Lozano, 2010). **Figure 2.2** shows such a structure. Moreover, classifying cloud computing services along with different layers is common practice in the industry.

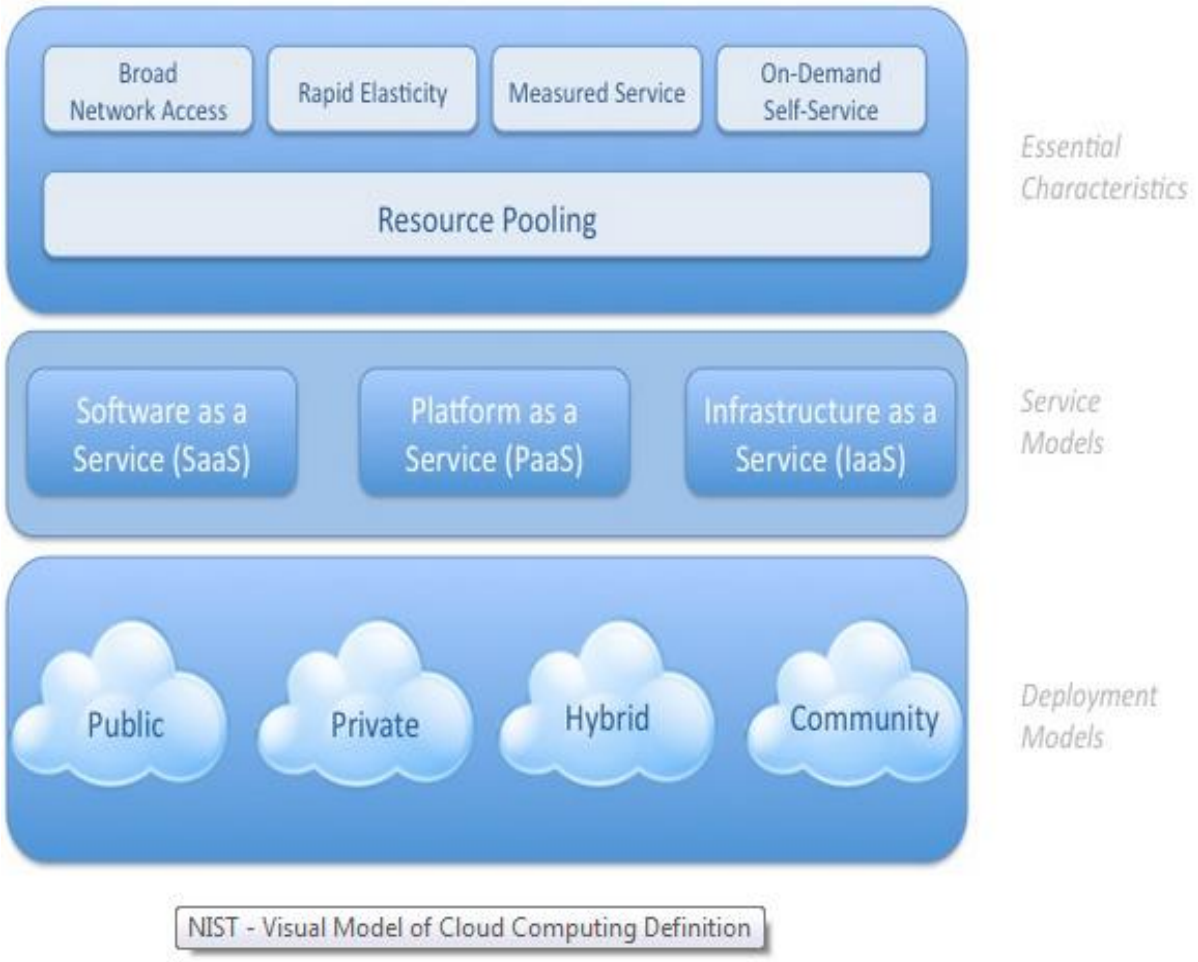


Figure 2.2- Illustration of Cloud Taxonomy [Adapted and Modified from (Mell & Grance, 2011)]

2.4 Cloud Computing Characteristics and Reference Architecture (CCRA)

In Figure 2, the NIST definition of cloud computing identifies five essential characteristics which are briefly discussed below:

1. *Rapid Elasticity:* is one of the essential characteristics common in cloud computing. Elasticity in cloud computing context is defined as the ability for consumers to scale resources both up and down as needed.
2. *Measured Service:* is crucial for billing, access control, resource optimization, capacity planning and other tasks. In a measured service, aspect of the cloud service is controlled and monitored by the cloud provider. Typically, metering is done on a pay-per-use or charge-per-use basis
3. *On-demand Self Service:* aspect of cloud computing means that a consumer can use services as needed without any human interaction with the cloud provider.
4. *Broad Network Access:* means that the cloud provider's capabilities are available over the network and can be accessed through standard mechanisms (e.g. http, xml, and/or internet protocols) by both thick and thin clients (e.g. mobile phones, tablets, laptops, and workstations). Note, this does not necessarily mean Internet access – regardless of the type of network, access to the cloud is typically not limited to a client. The term broad network access can apply equally to public, private, or hybrid clouds
5. *Resource Pooling:* allows a cloud provider to serve its customers via multi-tenant model (i.e. shared among more than one consumer). Physical and virtual resources are assigned per consumer demand. Resource pooling is an inherent benefit of any cloud service model (SaaS, PaaS or IaaS).

Cloud Computing Reference Architecture

Reference architecture provides a technical blueprint for a system with a well-defined scope, the requirements it satisfies, and the architectural decisions it realizes. It ensures consistency and quality across development and delivery projects (IBM, 2012). IBM's cloud computing reference architecture defines three main roles typically encountered in any cloud computing environment: the cloud service creator, cloud service provider, and cloud service consumer (Tobias et al, 2012). The Cloud Computing Reference Architecture (CCRA) depicted in **Figure 2.3** is a natural extension to the NIST cloud computing definition in preceding section. This diagram depicts a generic high-level architecture and is intended to facilitate the understanding of the requirements, uses, characteristics and standards of cloud computing (Liu et al. 2011). The CCRA is a powerful tool used for discussing the requirements, structures, and operations of cloud computing. It defines a set of actors, activities, and functions that can be used in the process of developing cloud computing architectures, well as

providing guidelines for creating a cloud environment. However, the CCRA focuses on the requirements of what cloud service provides, not on a design that defines a solution and its implementation. In other words, the reference architecture does not represent the system architecture of a specific system; instead, it is a tool for discussing, and developing the system-specific architecture (Hogan et al. 2011). The architecture defines five major actors: 1) cloud consumer, 2) cloud provider, 3) cloud auditor, 4) cloud broker, and 5) cloud carrier. However, due to significant role of a "cloud service developer" which has not been included in NIST CCRA, author has expanded the discussion in subsequent section to also include this role and related tasks (see **Figure 2.3**). Thus, an overview of the NIST-CCRA which includes a cloud service developer role and related responsibility is illustrated in a revised cloud computing taxonomy shown later in this thesis (refer to *Section 2.4.4*). Moreover, the functions of the six major actors in the CCRA have already been defined in sub-*section 2.4.3*. Each actor/role represents a person or an organisation that participates in a transaction or process and/or performs tasks in cloud computing. Notice that in **Figure 2.3**, open standards are needed for the interactions between these actors/roles. The reason is that activities to keep the cloud open and interoperable should be customer driven, and existing/open standards should be used wherever possible to make it possible to avoid vendor lock-in. The following section presents the different delivery mechanisms for cloud services.

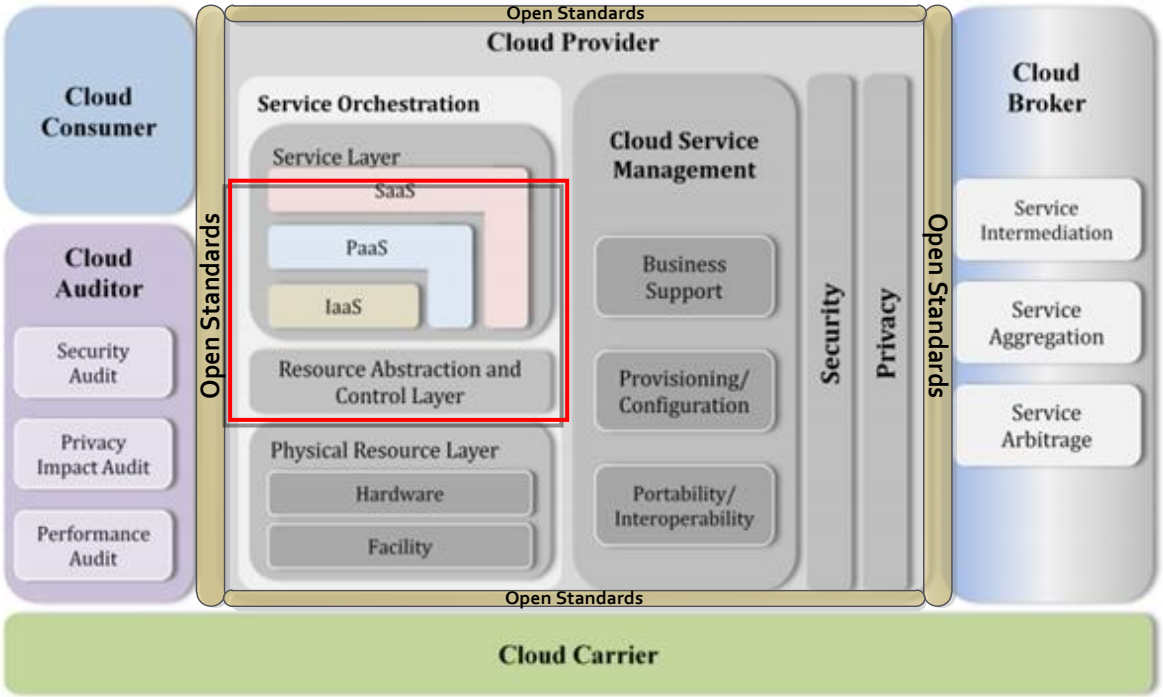


Figure 2.3- Cloud Computing Reference Architecture (CCRA) [Adapted and modified from (Liu et al. 2011)]

2.4.1 Cloud Service Models

Cloud service models describe how different types of IT services and resources are offered as a service by the cloud provider. In the commercial cloud market place, there is a wide range of available cloud service offerings that vary in complexity and value. As illustrated previously in **Figure 2.1**, this market place is organised into a general set of service categories layered in a notional stack, with foundational offerings found toward the bottom (e.g. cloud storage) and more complex offerings toward the top (e.g. cloud applications). The cloud service models described below are conformant to the NIST definition of cloud computing. Prior to presenting the different service models (i.e. **Figure 2.5**), a correlation between the cloud computing software stack and the different service models including the dependencies of cloud service offerings are depicted in **Figure 2.4a** and **Figure 2.4b**. Following system architecture conventions, the horizontal positioning, i.e., the layering, in a model represents dependency relationships – the upper layer components are dependent on adjacent lower layer. Due to the clouds' elastic and usage-based pricing model, often one service offering may require same properties to be present in underlying application layers. That is, a cloud service model may rely on other resources also offered as a service. It is possible, though not necessary, that SaaS applications (for instance) can be built on top of PaaS components and PaaS components can be built on top of IaaS components (Liu et al, 2011). The optional dependency relationships among SaaS, PaaS, and IaaS components (see **Figure 2.1** – service layer) are represented graphically as components stacking on each other; while the angling of the components represents that each of the service component can stand by itself. For example, a SaaS application can be implemented and hosted on virtual machines from an IaaS cloud or it can be implemented directly on top of cloud resources without using IaaS virtual machines. Thus, having a clear understanding of the dependencies between cloud computing models is critical to understanding the inherent cloud computing security and vendor lock-in risks. The NIST has already proposed the three main categories of cloud computing. The three service models are depicted in **Figure 2.5** and described below.

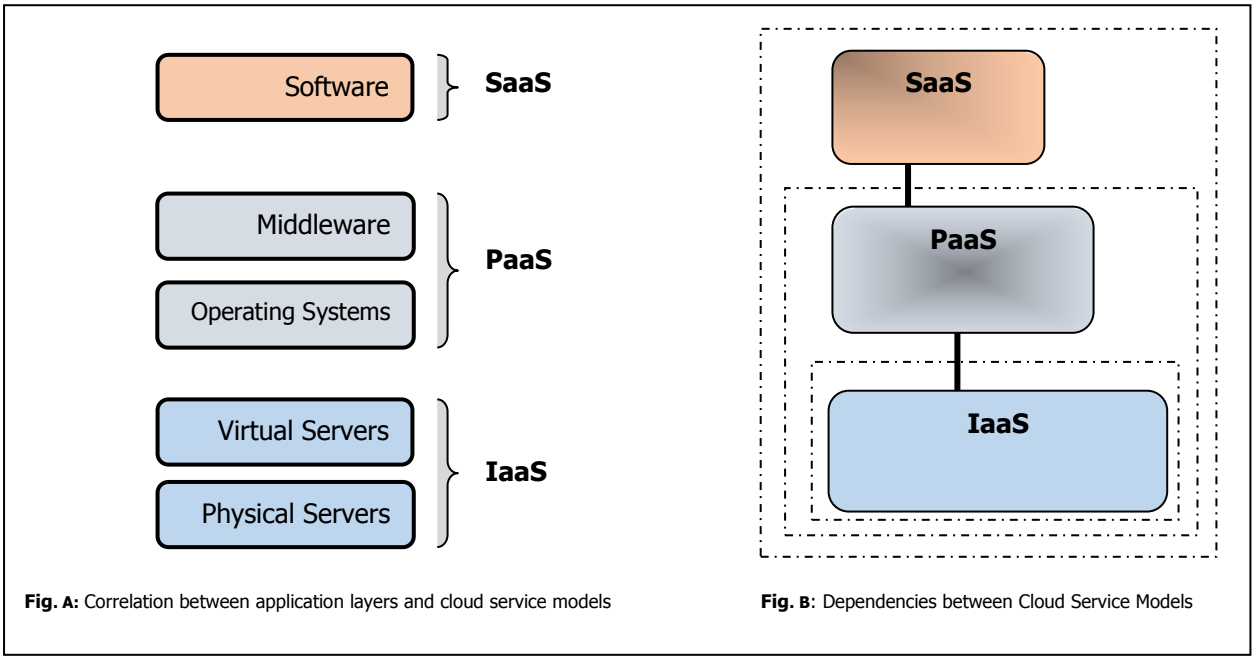


Fig. A: Correlation between application layers and cloud service models

Fig. B: Dependencies between Cloud Service Models

Figure 2.4- Correlations between cloud service models and their dependencies

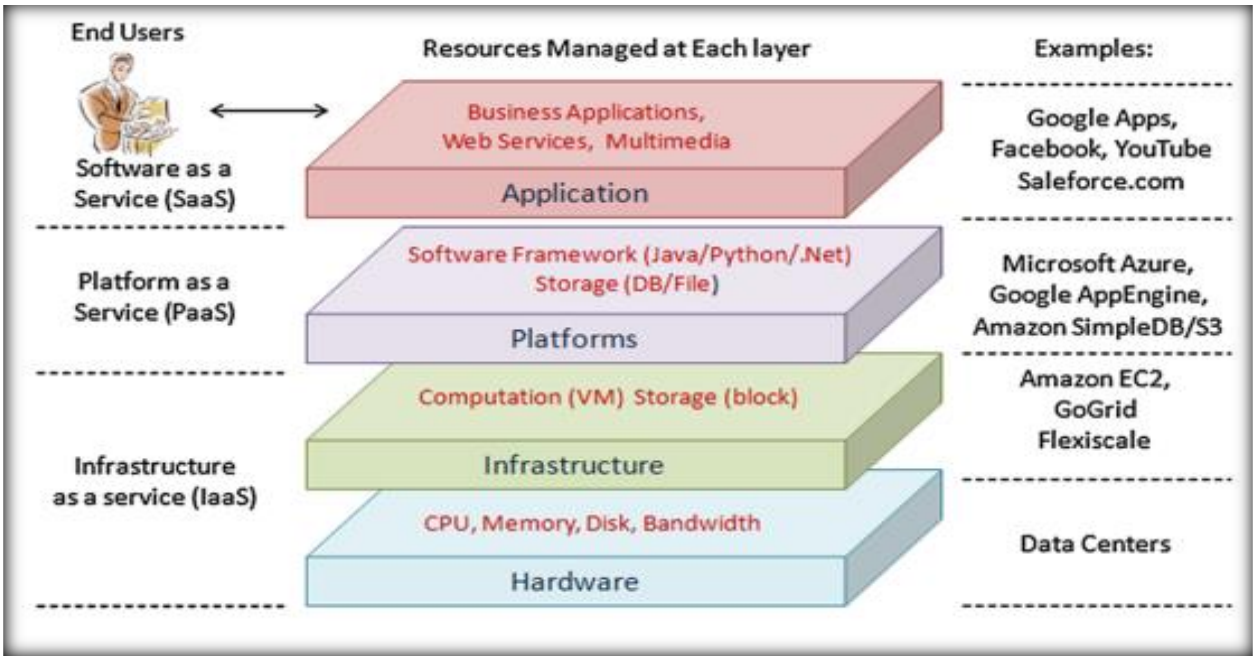


Figure 2.5- Three main categories of cloud computing [Adapted from (Zhang, Cheng & Boutaba 2010)]

Infrastructure as a Service (IaaS) is a model in which IT infrastructures ranging from CPU power to storage are exposed as resource over the Internet. Cloud users can dynamically align their infrastructure per their needs, while resources are provided on demand. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage

deployed applications, and possibly limited control of select networking components (e.g. host firewalls).

Platform as a Service (PaaS) consists of application development platforms, remotely accessible through the web and able to connect to locally executed frameworks and IDEs, allowing fast development and deployment of applications. The consumer does no manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly application hosting environment.

Software as a Service (SaaS) allows providers to expose stand-alone applications, running on a distributed cloud infrastructure completely hidden from customers, as resources through the Internet. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, except for limited user-specific application configuration settings.

- **Service Model Specific Characteristics**

Having previously discussed the essential characteristics of cloud computing in *Section 2.4*, a similarity between all cloud service models is the delivery and provision of cloud offerings in a flexible and abstracted way (Kachele et al. 2013). The cloud service models are best distinguished by two factors: 1) the computing capability that is provisioned (e.g. Software Application, Platform or Infrastructure); and 2) the primary consumers (i.e. end-users, developer, deployer, or IT operations). Besides, an essential characteristic (i.e. broad network access) is observed to be supported differently by nature of the computing capability provisioned. For example, the term "applications" in the SaaS context refers to cloud-enabled applications (e.g. Web or mobile), while the terms "platform" and "applications" in the PaaS context refers to development and/or deployment platform for cloud-enabled applications by nature of supporting essential characteristic (i.e. broad network access). This differs from VM/desktop software and applications that may be installed on a virtual machine. The resulting observation shows that more specific features of infrastructure, platform, and software application cloud services do not allow clear distinctions within the chosen characteristics. Therefore, author identifies and presents only a few service-specific characteristics below:

1. *IaaS-specific characteristics:* A characteristics to consider are the supported operating systems and applications/frameworks, as this might be important to potential customers. Most IaaS providers support Linux systems, but some also have Windows and OpenSolaris support. Widely supported applications include the MySQL database and the Apache HTTP Server software. Another characteristic that is important for developers is whether and what kind of development tools the provider supplies. This could include an API or special command-line

tools (Tippit, 2012). Services comprising virtual instances can be further differentiated based on the virtualization technology used. Xen (Citrix, 2016), is currently used by most providers.

2. *PaaS-specific characteristics:* An important PaaS characteristic is related to which programming languages and platforms are supported. Google's App Engine, for example, currently only supports Python and Java environments. The supported operating systems and applications can also be a relevant feature.
3. *SaaS-specific characteristics:* Software cloud services vary a lot. A characteristic to consider is the customer/application domain of the offered service. This domain could be customer relations or other business management areas, office applications, social networking, and data exchange.

2.4.2 Cloud Service Types

Like in the case of service models, different types of clouds exist that can mainly be distinguished by the institution they are associated with – i.e. the organisation that is responsible for the operation of the cloud, and the targeted user group. Cloud service types (also referred to as deployment models) can be categorised based on the control and sharing of physical or virtual resources. A cloud computing infrastructure may be operated in one of the following deployment models:

Private Cloud: The cloud infrastructure is operated solely for an organisation. It may be managed by the organisation or a third party and may exist on or off premise.

Public Cloud: The cloud infrastructure is made available to the general public or a large industry group and is owned by an organisation selling cloud services.

Community Cloud: The cloud infrastructure is shared by several organisations and supports a specific community that has shared concerns (e.g. mission, security requirements, and policy and compliance considerations). It may be managed by the organisations or a third party and may exist on premise or off premise.

Hybrid Cloud: The cloud infrastructure is a composition of two or more clouds (i.e. private, community or public) that remain unique entities but are bound together by standardised or proprietary technology that enables data and application portability (cloud bursting for load balancing between clouds).

The scope of control of resources in a cloud system is shared between the cloud provider and cloud consumer. As illustrated in **Figure 2.6**, this analysis of delineation of controls over the application stack increases understanding of the responsibilities of parties involved in managing the cloud application (Badger et al. 2011).

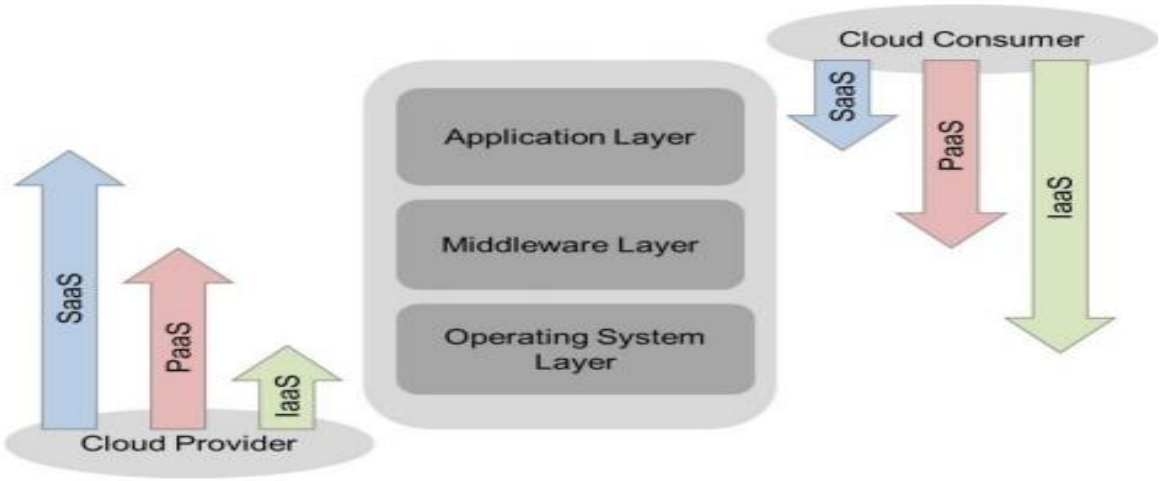


Figure 2.6- Scope of Control between Cloud Provider and Consumer (Badger et al. 2011).

2.4.3 The Sub-services of Cloud Computing

A cloud computing system offers different services following different cloud service models. Based on the three primary types of cloud service models discussed earlier in *Section 2.4.1*, other specific set of sub-services have emerged to describe different specialisation of the aforesaid. The sub-services are informally referred to as 'cloud sub-service marketing terms' which are often coined and used by industry by simply adding the suffix "aaS" after a computing capability (e.g. Hardware as a Service). Cloud sub-service terms do not replace the three service models (SaaS, PaaS and IaaS), which serve as the high-level categorisation of cloud services, but rather serve to informally facilitate communication relating to specialised services. The cloud sub-service types discussed in this section concisely explain the nature and behaviour of these specific services. The services in these categories can include capabilities from one or more of the three main types of cloud capabilities type (refer to *Section 2.4.1*). Some notable sub-services are described below:

STorage as a Service (STaaS) has been increasing in popularity recently due to many of the same reasons as cloud computing. A storage cloud capability provides storage as a service (STaaS) to storage consumers, where they pay based on the amount of storage space used. It can be delivered in any of the previously discussed cloud delivery models (i.e. public, private, hybrid, and community). Cloud storage as a service delivers virtualised storage on demand, over a network based on a request for a given quality of service (QoS) (Coyne et al. 2016). It can be used to support a diverse range of storage needs, including mass data stores, file shares, backup, archive etc. Implementations range from public user data stores to large private storage areas networks (SAN) or network-attached storage (NAS), hosted in-house or at third-party managed facilities. A SaaS cloud can be used in various ways, based on an organisation's specific requirements.

Hardware as a Service (HaaS) was coined possibly in 2006. As the result of rapid advances in hardware virtualization, IT automation and usage metering and pricing, users could buy IT hardware, or even an entire data centre, as a pay-as-you-go subscription service. The HaaS is flexible, scalable and manageable to meet a consumer enterprise needs. Examples could be found at Amazon EC2, IBM's Blue Cloud project, Nimbus, Eucalyptus and Enomalism.

Compute Capacity as a Service (CCaaS) is the provision of raw computing resource, typically used in the execution of mathematically complex models from either a single supercomputer resource or a large number of distributed computing resources where the task performs well.

Composite as a Service (CaaS) layer of the cloud computing stack includes the definition of software components run in a distributed fashion, across the Internet with defined service interfaces as a basis for system-to-system integration. In this model, different provider supplied services are offered to users that are isolated from each other on a pay-per-use basis. These users are enabled to create individual compositions of provider supplied services to meet their functional and service level requirements. The ability to compose one cloud service from one or more other cloud services is based on the principle of composability adopted from SOA. As such, the body of research on SOA has numerous studies on composable IT services which have direct application to providing and composing SaaS (Youseff et al. 2008). While CaaS is still an ongoing research, a good introduction to its relation to IaaS, PaaS and SaaS are given in (Rosenberg, 2010; Leymann, 2009). Rosenberg (2010) describes the importance of CaaS during the adaptation of software and its reconfiguration. Moreover, today, CaaS is already offered as online platforms that allow modelling and execution of business processes, such as RunMyProcess (2015), Cordys Process Factory (2015) etc.

Business Process as a Service (BPaaS) is an IBM-specific definition. This model combines software and workflow elements to deliver end-to-end business processes as a service. BPaaS are any business process (horizontal or vertical) delivered through the cloud service model (multi-tenant, self-service provisioning, elastic scaling and usage meeting or pricing) through the Internet with access via web-centric interfaces and exploiting web-oriented cloud architecture. Horizontal applications such as payroll, technical support, and billing, as well as vertical markets like healthcare and insurance can be delivered through this model. BPaaS allows businesses to pass on some of their day-to-day operating costs to service providers y using a fee-for-service model so that businesses can focus on their core competencies (Coyne et al. 2016). The BPaaS provider is responsible for the related business function(s). Examples of commercial implementations of BPaaS include IBM source to pay on cloud, IBM customer experience on cloud, IBM Watson business solutions and Google AdSense.

2.4.4 Cloud Computing User Roles

In the following section, we describe the major actors/role of cloud computing previously identified in *Section 2.4*. A role is a set of cloud computing activities that serve a common purpose. For a more comprehensive and detailed high-level descriptions of all cloud computing roles, sub-roles and their various related-activities, please refer to the ISO/IEC 17789 cloud computing reference architecture standard (ITU-T, 2014). **Figure 2.7** shows the roles of cloud computing, with their associated sub-roles. The sub-roles of the cloud service customer (or consumer) and the cloud service provider are involved in the split of responsibilities that is typical for enterprise cloud services. Therefore, it becomes important for cloud service consumers to understand the key activities and responsibilities of the various sub-roles. This will ensure that the cloud service agreement and its associated service level agreement contain appropriate commitments and service level targets to address those activities and responsibilities for the cloud service covered by the contract.

Cloud Service Consumer (or customers): A cloud service consumer (or customer) is a person, organisation or an IT system that maintains a business relationship with, and uses service from, cloud providers. Service level agreements (SLAs) specify the requirements fulfilled by a certain or a set of services, to let consumers, choose the appropriate ones. Besides IT capabilities consumed as cloud services, consumers may continue to have in-house IT managed in a traditional non-cloud fashion. The role of the cloud consumer slightly changes when comparing the NIST CCRA to IBM CCRA. For instance, in IBM CCRA, the consumer has more control over the consumed services with the possibility to integrate with existing in-house IT (Behrendt et al. 2011). However, depending on the services requested the activities and usage scenarios can be different among cloud consumers, as described below and shown also in **Table 2.1**. **Figure 2.8** presents some example of cloud services available to a cloud consumer.

Consuming Cloud Services at Different Abstraction Layers

- SaaS applications are usually deployed as hosted services in the cloud and are made accessible via a network connecting SaaS consumers and providers. The consumers of SaaS can be organizations that provide their members with access to software applications, end users who directly use software applications, or software application administrators who configure applications for end users. SaaS consumers can be billed based on the number of end users, the time of use, the network bandwidth consumed, and the amount of data stored or duration of stored data.
- Cloud consumers of PaaS can employ the tools and execution resources provided by cloud providers to develop, test, deploy and manage the applications hosted in a cloud environment. PaaS consumers can be application developers who design and implement application software, application testers who run and test applications in cloud-based environments,

application migration specialists who publish applications into the cloud, and application administrators who configure and monitor application performance on a platform. PaaS consumers can be billed per, processing, database storage and network resources consumed by the PaaS application, and the duration of the platform usage.

- Consumers of IaaS have access to virtual computers, network-accessible storage, network infrastructure components, and other fundamental computing resources on which they can deploy and run arbitrary software. The consumers of IaaS can be system developers, system administrators and IT managers who are interested in creating, installing, managing and monitoring services for IT infrastructure operations. IaaS consumers are provisioned with the capabilities to access these computing resources, and are billed per the amount or duration of the resources consumed, such as CPU hours used by virtual computers, volume and duration of data stored, network bandwidth consumed, number of IP addresses used for certain intervals.

Table 2.1 Cloud Consumer and Cloud Provider activities

Type	Consumer Activities	Provider Activities
SaaS	Uses application/service for business process operations.	Installs, manages, maintains, and supports the software application on a cloud infrastructure.
PaaS	Develops tests, deploys, and manages applications hosted in a cloud environment.	Provisions and manages cloud infrastructure and middleware for the platform consumers; provides development, deployment, and administration tools to platform consumers.
IaaS	Creates/installs, manages, and monitors services for IT infrastructure operations.	Provisions and manages the physical processing, storage, networking, and the hosting environment and cloud infrastructure for IaaS consumers.

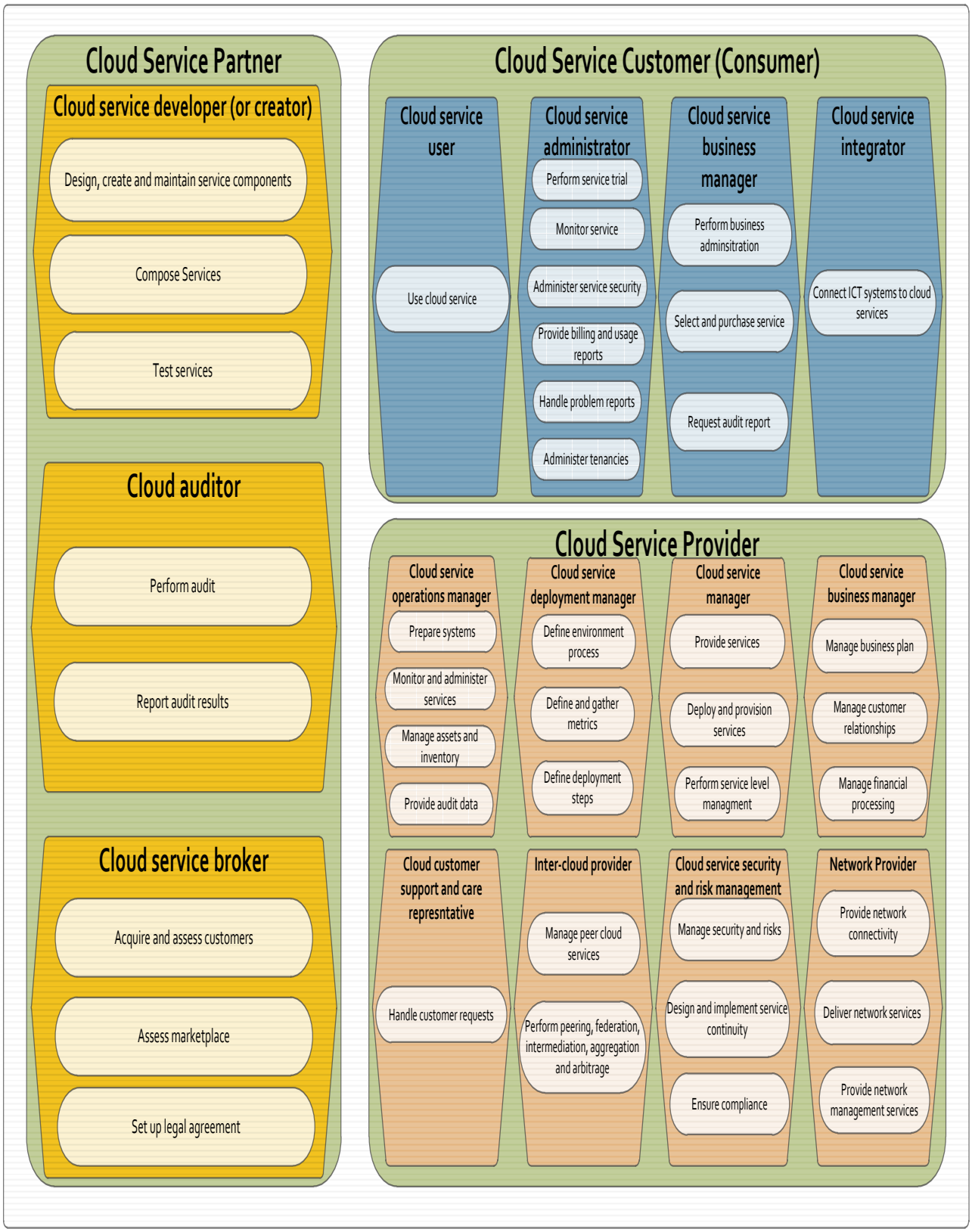


Figure 2.7- Cloud Computing Roles, Sub-roles and Related Activities

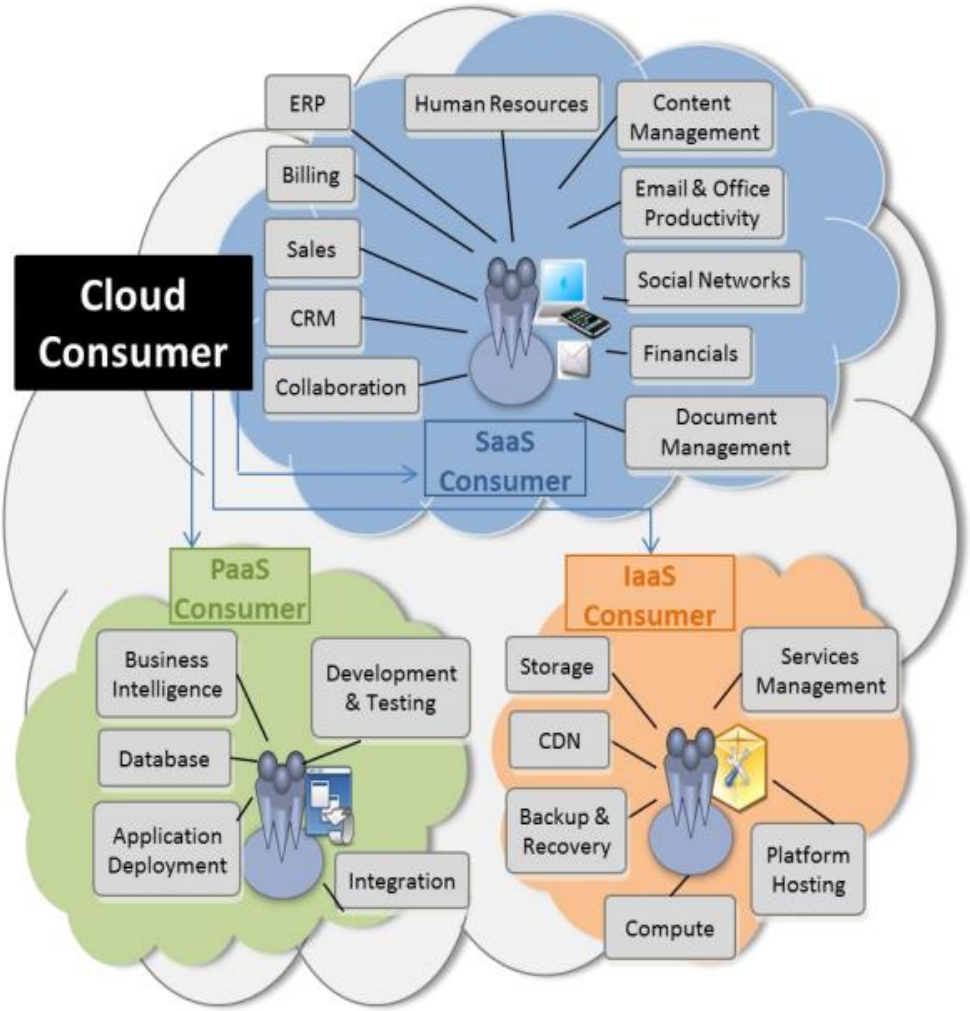


Figure 2.8- Example of Business IT services available to a cloud consumer [Adapted from (Pritzker and Gallagher, 2013)]

Cloud Service Provider: represents either a person or an organisation offering cloud services to cloud consumers. It is the cloud provider's responsibility to build the requested software/platform/infrastructure services, provisions the services at agreed-upon service levels, and protects the security and privacy of the services. Those services are delivered by a Common Cloud Management Platform (CCMP) either by running CCMP infrastructure or consuming one as a service (Stifani et al. 2012). The cloud service provider is responsible for dealing with the business relationship with cloud service customers. As described in Table 1, cloud providers undertake different tasks for the provisioning of various service models. A cloud provider's activities can be described in five major areas shown in **Figure 2.9**. The activity areas in which cloud providers are involved concerns service deployment, service orchestration, cloud service management, security and privacy (Martino et al. 2015). For full analysis of these areas, please refer to the work by (Liu et al. 2011).

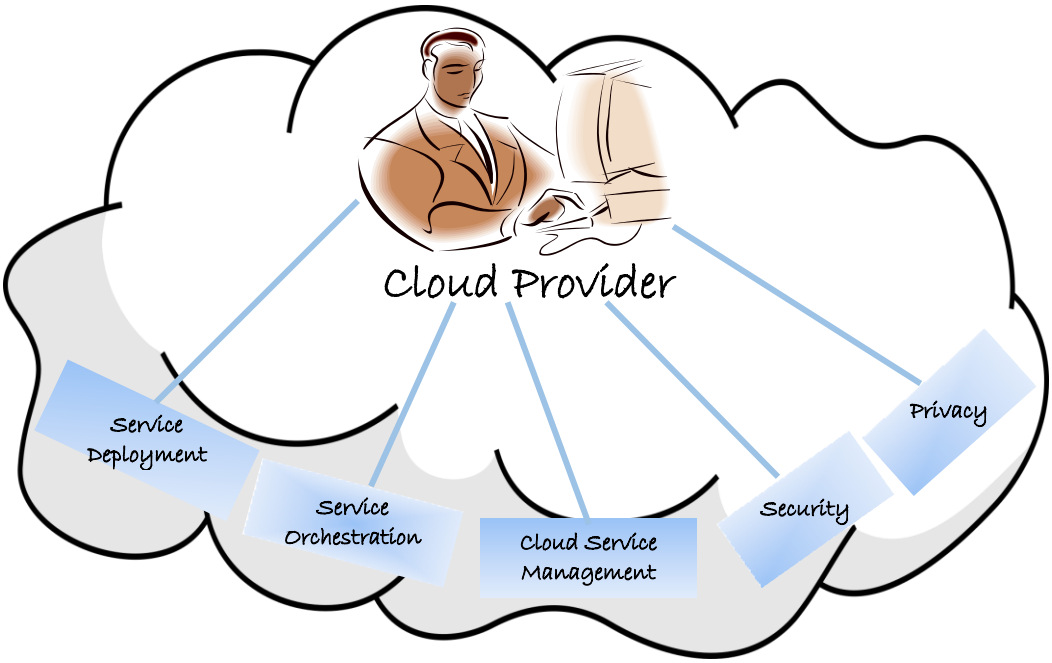


Figure 2.9- Major activities of a Cloud Provider

Cloud Service Developer (or Creator): A cloud service developer is a sub-role of cloud service partner which is responsible for designing, developing, testing and maintaining the implementation of a service. The cloud service developer creates, publishes and monitors the cloud service. These are typically "line-of-business" applications that are delivered directly to end-users via the SaaS model. Hence, applications written at the IaaS and PaaS levels will subsequently be used by SaaS developers and cloud providers. Development environments for service creation vary. If developers are creating a SaaS application, they are most likely writing code for an environment hosted by a cloud provider. In this case, publishing the service is deploying it to the cloud provider's infrastructure. During service creation, analytics involve remote debugging to test the service before it is published to consumers. Once the service is published, analytics allow developers to monitor the performance of their service and make changes as necessary (Ahronovitz et al. 2010). In the IBM CCRA, the service developer is also referred to as "Cloud Service Creator." Service development tools are used by the cloud service creator to develop new cloud new cloud service definitions, including runtime artefacts and management-related aspects (such as monitoring, metering, provisioning, etc.) (Stefani et al. 2012). The cloud service developer's activities include design, create and maintain service component, test service, compose services (see **Figure 2.7**).

Cloud Auditor: The cloud auditor is a sub-role of cloud service partner with the responsibility of conducting an audit of the provision and use of cloud services. The auditor performs independent assessment and examinations of cloud services, information system operations, performance, and security of a cloud implementation. A cloud audit typically covers operations, performance and security, and evaluates the services of a cloud provider to verify conformance to standards or whether

a specified set of audit criteria are met in terms of fulfilment of the SLAs. The cloud auditor's activities (as depicted in **Figure 7**) include: perform audit and report audit results.

Cloud Service Broker: The cloud service broker is a sub-role of cloud service partner that negotiates and/or manages service negotiations and relationships between cloud consumer and providers, acting as an intermediary. The cloud service broker is not itself a cloud service provider and should not be confused with the role of inter-cloud provider either. However, the cloud service broker role could be combined with or operate independently of the role of inter-cloud provider. As cloud computing evolves, the integration of cloud services can be too complex for cloud consumers to manage. A cloud consumer may request services from a cloud broker, instead of contacting the cloud provider directly. In general, a cloud broker can provide services in three categories: 1) service intermediation, 2) service aggregation, and 3) service arbitrage (Mell and Grance, 2011).

Cloud Carrier: provides connectivity and transport services, enabling consumers to access the selected services through different communication devices, generally represented by the Internet. Cloud consumers can obtain cloud services through network access devices, such as computers, laptops, mobile smart phones and tablets etc. The distribution of cloud services is normally provided by network and telecommunication carriers.

Cloud Service Partner: A cloud service partner is a party which is engaged in support of, or auxiliary to, activities of either the cloud service provider or the cloud service customer, or both. A cloud service partner's cloud computing activities may vary depending on the type of partner and their relationship with the cloud service provider and the cloud service customer. Note that a cloud service customer can also have a business relationship with a cloud service partner for a variety of purposes.

2.4.5 Taxonomy of Cloud Computing

Taxonomy is the science of categorization, or classification, of things based on a predefined system and typically, contains a controlled vocabulary with a hierarchical tree-like structure (Liu et al. 2011). **Figure 2.10** presents taxonomy associated with cloud computing reference architecture (CCRA) discussed earlier in *Section 2.4*. This four-level taxonomy is adapted and refined to describe the key concepts of cloud computing from the preceding section. Note that the adaptations include the role of a service developer (i.e. service creator) as well as other sub-categories. The roles and components refined have been highlighted in black/grey. The levels within the defined taxonomy include:

- *Level 1: Role,* which indicates a set of obligations and behaviours as conceptualized by the associated actors in the context of cloud computing.
- *Level 2: Activity,* which entails the general behaviours or tasks associated to a specific role.

- *Level 3: Component,* which refer to the specific processes, actions, or tasks that must be performed to meet the objective of a specific activity.
- *Level 4: Sub-component,* which present a modular part of a component.

For more detailed information about each level of the taxonomy depicted in **Figure 2.10**, please refer to the works of (Liu et al. 2011 and Ahronovitz et al. 2010). Before examining relevance of the revised taxonomy and why it has been used within this thesis, remember in *Section 2.4.3,* a diagram (see **Figure 2.7**) was presented earlier to illustrate and understand the fundamental cloud computing actors, user role, and sub-roles. In view of **Figure 2.7**, the improved taxonomy presented in this section can be used as a tool to examine a cloud service lifecycle, discuss the (shared) responsibility and interactions between the actors, facilitate the analysis of potential standards for security, interoperability, portability, and provide a clearer picture of the architectural components in the NIST CCRA.

The high-level taxonomy diagram provides an effective strategy for describing cloud computing activities, shared issues across the roles, sub-roles, as well as the functional architecture and components of cloud computing. The functional component in this context represent sets of functions that are required to perform the cloud computing activities (refer to *Level 2* in **Figure 2.10**) for the various user roles and sub-roles (see **Figure 2.7**) involved in cloud computing as described in *Section 2.4.3*. In summary, the concise discussion and information provided in this introduction to cloud computing covers the basic notions needed to clearly apprehend the following sections and remaining chapters of this thesis. The next section discusses cloud application architecture principles with a emphasis on cloud application software capabilities (i.e. SaaS) type.

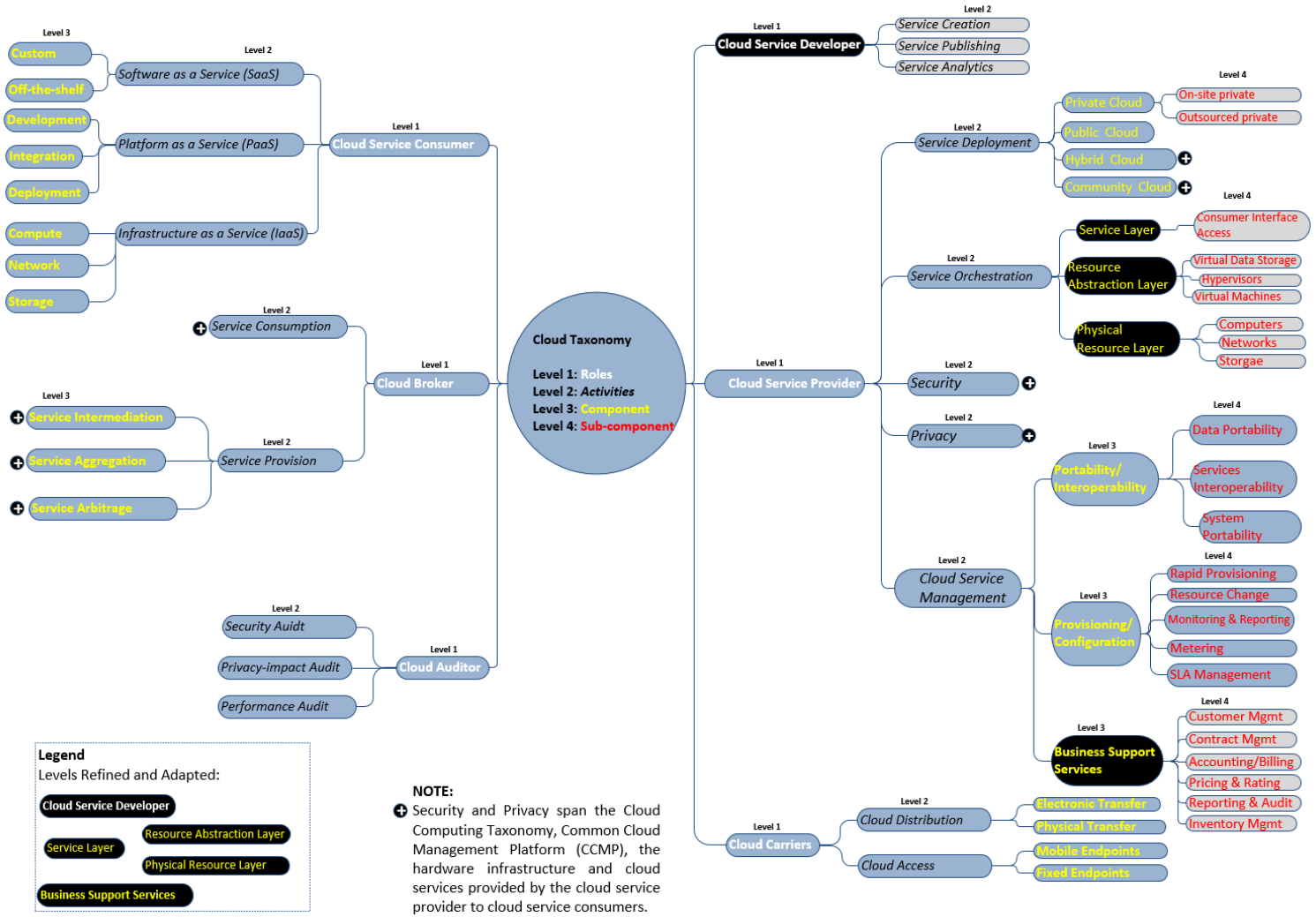


Figure 2.10-Cloud Computing Taxonomy: Adapted and modified from (Liu et al. 2011)

2.4.6 Using Cloud Services and Engaging with Cloud Customers

Cloud computing is about providing services. A service has a provider and a consumer. It exposes the capability that the provider has that is of value to the consumer. The cloud provider of a cloud service has control over a set of resources (e.g. processors, data stores, system programs, applications programs, and networks), and makes them available to consumers of service under a contract. An example is the case when a company, for instance, buys SaaS from a cloud provider and uses that service(s) to support its business operations. The cloud SaaS provider hosts the application centrally and delivers access to multiple customers over the Internet in exchange for a fee. This creates an opportunity for enterprise IT departments to change their focus from deploying and supporting applications to managing the services that those applications provide. Still, the adoption of cloud computing services has been impacted by challenges such as vendor lock-in, security, interoperability, portability, and service level agreement issues. These system-wide issues have an impact on different roles (i.e. stakeholders) involved in a cloud computing system. Thus, it represents shared concerns that need to be tackled when adopting, implementing, designing, and migrating to a cloud computing system. The rate at which enterprise organisations embrace cloud computing services is perhaps linked to the perceived immaturity and instability (i.e. due to technical incompatibilities) of the cloud services on offer from current cloud computing providers. Therefore, assessing the maturity level of cloud services using the revised taxonomy presented in **Figure 2.10** is one qualitative approach to achieve this. Further, the maturity of a cloud computing environment provides adopting organisations with an understanding of the suitability of the cloud service and the level of investment required by the cloud service customer to address the system-wide challenges around vendor lock-in, security etc.

- **Engaging with Cloud Consumers**

In many cases, a cloud consumer may request cloud services (i.e. SaaS, PaaS, or IaaS) from a cloud provider directly or via a cloud broker. Being that the cloud consumer is the ultimate stakeholder that the cloud computing service is created to support, a cloud consumer browses the service catalogue from a cloud provider, requests the appropriate service, sets up service contracts with the cloud provider, and uses the services as stipulated in the agreed upon cloud service agreement. The cloud consumer is either billed for the service or payments arrangements (e.g. monthly subscription, yearly, etc.) are made accordingly. In cloud computing, a specific well-defined interface is used to create an abstraction of the underlying implementation of the service which provides the supported functionality. An interface (or a specification that a cloud service publishes to customers) represents the primary mechanism by which the cloud service can be accessed. In as much as the interface does not change, the underlying implementation of a cloud service can be modified by a vendor without affecting any existing clients. Currently, many cloud providers offer their service through proprietary Application Programming Interfaces (APIs). Portability and interoperability is likely to be

increasingly important as the number of cloud providers increases. However, if an API to a cloud service is an open standard, one implemented by multiple vendors, a customer can choose to access any of those offerings without making major changes to their clients. For example, end-users that consume a cloud SaaS offering will place the most importance on the user interface of that offering and what features it supports. Whereas software developers on the other hand will focus on specific APIs that a PaaS platform supports, while IaaS consumers will focus on what hypervisors, virtual machines and operating systems are supported by an IaaS platform. Therefore, the value chain for any cloud infrastructure, platform, and software application is directly proportional to the compatibility and interoperability of the interfaces it supports. To represent the value offered by each given cloud service type and interface level, **Table 2.2** compares the different cloud models and what elements drive competition as well as what may hinder competition.

Table 2.2 Different Types of Cloud Services have Different Interface of Interest

Service Model Type	Main Interface(s) Level	Interface Target Audience & Functions	Value Provided by the Interface	What Drives Competition	What Hinders Competition
SaaS	Human (consumer)	End-users – use the features provided but do not manage the application	Automates provisioning, deployment and management of application functionality	Feature set, open file/document formats, consistent user interfaces, ability to export data to competitive offering(s).	Proprietary formats and protocols, dependencies on proprietary services, lack of data export capability.
PaaS	Software frameworks	Developers – use the interface to manage the service or the application, not the server	Automates provisioning, deployment, management and scaling of underlying operating system and hardware	Open source/open standards; multiple choice of programming languages, tools, scaling	Proprietary APIs, tools, frameworks; dependence upon proprietary platforms.
IaaS	Operating Systems (hardware resources)	IT Professionals and developers – use the interface to manage the cloud service, the application and the virtual hardware	Automates provisioning and deployment of physical hardware resources for virtual machines	Open source/open standards; cost, functionality.	Proprietary APIs, proprietary hypervisors, limited operating system support.

2.5 Cloud Computing and Software as a Service (SaaS) Application Architectures

Cloud computing services are increasingly being adopted in many areas, such as banking, e-commerce, retail industry, and academia. But sourcing strategy for such cloud services is often an afterthought. With the rapid rise in cloud computing, enterprise software as a service (SaaS) usage is

particularly in demand, as companies see benefits such as business agility, rapid time-to-market value, and the subscription model. For example, health informatics can help medical researchers diagnose challenging diseases and cancers (Jha et al. 2009). Financial analytics can ensure accurate and fast simulations to be available for investors (Peng et al. 2013). Education as a Service improves the quality of education and delivery (Mircea and Andreescu, 2011). Mobile applications allow users to play online games and easy-to-use applications to interact with their peers. This model still requires specialised staff resources that have the knowledge to manage a technical contract and work with the SaaS provider to ensure service is provided as expected. SaaS has several attributes which include but is not limited to accessibility, reliability, configurability, scalability, costs and standardised IT based capability. Cloud SaaS services come with shorter implementation time (and lower failure risks) compared to the conventional enterprise software implementation process. However, despite the cost benefits which are attractive for SaaS consumers, there are still concerns such as portability, ease of integration, customisation and functionality. For example, survey conducted by ENISA and Mimecast regarding cloud computing have shown the main concerns with SaaS adoptions are security, loss of data control, data lock-in, application lock-in, API lock-in, switching costs, data protection and compliance with government regulations (ENISA, 2009a; ENISA 2009b; Mimecast, 2010). It is suggested that cloud SaaS consumers should consider having consumer-managed security controls such as encryption and identity management (Tan et al. 2013). Moreover, while more consumers and enterprises use the cloud SaaS services, security and privacy become important to ensure that all the data they use and share are well protected. The hybrid SaaS delivery model has arisen in response to the aforesaid drawbacks, and may be the most appropriate model for consumer organisations with security, privacy and compliance related issues. Hybrid SaaS model allows the cloud service customer to deploy the solution as a SaaS service or as on-premise solution, with the ability to switch from one to the other as needed. If deployed as a SaaS service the application may be hosted by a SaaS provider, as a Multi-tenanted application, and a separate database is located at each tenant to ensure data security. Thus, moving to a SaaS cloud model means taking a few considerations into account, each of which ultimately boils down to a tension between control and cost. Some of which include political, technical, financial and legal considerations (Chong and Carraro, 2006). On some occasions, technical and financial considerations also can have legal ramifications, such as whether potential cloud SaaS providers will be able to meet the internal standards for data security and privacy to avoid legal exposure. Thus, from the consumer of a SaaS perspective, it is important to consider any legal obligations toward customers or other parties, and whether SaaS will allow the consumer organisation to continue to meet them. Furthermore, SaaS consumers should consider the legislations which govern the interception and disclosure of their data for all jurisdictions in which their data are stored and transmitted across to ensure contractually agreed standards are met.

In the context of software as a service, there are three types of primary SaaS stakeholders (i.e. user roles) identified (Anderson and Young, 2010):

- **IT Users**: Primary IT user roles within SaaS clouds are application administrators and SaaS specialists. The administrator is responsible for the decision to use SaaS for an application and for any integration work needed to deliver the service in the cloud. The SaaS specialist on the other hand, is the technical resource who delivers any personalisation, and customisation for an organisation.

- **SaaS Provider**: This is the external provider that delivers a software service over the Internet via cloud computing technologies to consumers. The provider comprises the SaaS infrastructure provider and SaaS provider. SaaS infrastructure provider owns and manages cloud computing resources (which include hardware, network and system software) – for example, Amazon, IBM and Oracle. Whereas, the SaaS provider serves the front-end SaaS consumers usually by using software running on hardware-software resources managed by a SaaS infrastructure provider. Moreover, it is possible that the SaaS infrastructure provider and SaaS provider is the same vendor.

- **SaaS End-Users**: This is classified as the primary end-users or individual workers who use SaaS applications for job-related activities. These end-users or individual workers are located within the enterprise or connected to cloud while travelling or working from home.

From the above paragraphs, we have seen that many reasons exist for utilising a solution provided through SaaS deployment model within enterprise IT environments. Unfortunately, too often the benefits are not properly weighted against the challenges of integrating data between a SaaS provider and the data within a company's existing ICT systems. These issues stem from a combination of factors that cut across organisational boundaries such as security, interoperability, management, regulatory compliance etc. With the growing availability of many SaaS solutions, organisations desire common integration methods and services to support agility and the rapid proliferation of new capabilities. To enhance the understanding of SaaS systems and support the consumer and solution developer (or creator) on how to create, design, and deploy solutions that are secure, open, multi-vendor and interoperable, we have identified specific areas and features for cloud SaaS architectures. The identification of factors used in feature model of cloud computing SaaS architectures is based on a commonality and variability analysis study. To formulate the feature models, author have analysed SaaS industry trends and scanned for existing SaaS implementation to gather best known methods and architectural techniques. The SaaS architectural feature defines the components and capabilities required for deployment, integration and a vocabulary for consistent communication with cloud SaaS providers. The review of architectural features for cloud-based applications has been based on an extensive systematic literature review on cloud computing and

SaaS architectures (OPDCA 2014; OPDCA 2012; Spence, 2009; Joshi, 2009; Carraro and Chong, 2008; Laplante et al. 2008). Hence, author focuses more on SaaS architecture features in the cited sources. In general, when describing SaaS, no specific application architecture or framework is prescribed but rather the general components and structure is defined. An appropriate SaaS architecture design will play a fundamental goal in supporting the cloud computing goals (Ozturk et al., 2011; Clements et al. 2010; Laplante et al. 2008). Moreover, how to choose a desired cloud SaaS service from the pools of candidate services is becoming an increasingly important research issue (Sun et al. 2013). Selecting the best cloud SaaS service based on consumer's preference is a complex problem due to the multiple consumer requirements (Silas et al. 2012). Enterprises need to adopt an objective approach to ensure they select the most appropriate SaaS product for their needs. The goal is to facilitate the shift from mere subjective evaluation to prescriptive deployment and selection of SaaS applications from cloud providers, with greater consistency among implementations and reduced implementation effort. In turn, this will support the advancement of software as a service migration and cloud computing adoption, in general. This selection issue is further explored in *Section 3.8.1* of this thesis.

2.5.1 Portability and Interconnectability of SaaS Environments

Moving to a SaaS cloud or changing SaaS vendors within the cloud is impacted by architecture differences. Systems in the cloud may reside in disparate platform architectures. Leading cloud platforms such as Google App Engine (GAE), Force.com, IBM Bluemix, and Amazon all provide some degree of support for moving applications and data components. However, each vendor cloud platform or solution offerings is architected differently enough so that the move from one to another is not easy but prone to errors. Appropriate portability assessments must be made to plan for adjustments required to ensure both data portability and application interconnectability (i.e. platform interoperability) and are maintained.

- **Configuration Management for SaaS using IaaS Tools**

Services (consumed as SaaS or) moved from traditional IT environments to cloud-based solutions can be expected to lack integration points with existing management tools used to monitor, report, and remedy system faults. Managing SaaS applications using IaaS tools becomes much more difficult with a move to the cloud. Traditional IT management tools operate effectively within the established enterprise boundary, but they lack the ability to manage services as they move outside the perimeter into the cloud environment. Thus, it becomes important to monitor internal as well as external application(s) interfaces regardless of location. It is crucial also to understand what management control capabilities are provided by a selected service provider interface and be prepared to adopt a set of new management tools to maintain hosted functions. This can result in supporting more than one management tool to cover internal and external systems. In the provisioning of a SaaS application,

various stakeholders with different objectives are involved, i.e., providers of all cloud stack layers as well as tenants and their users (Mell and Grance, 2011; Schroeter et al. 2012a). Therefore, to provide a highly configurable cloud SaaS application for a large number of tenants and their associated users in a shared cloud environment demands for a dynamic, yet scalable configuration management tool to support for multiple stakeholders (Schroeter et al. 2012b). Since today's software systems have many dependencies, development and operation teams have to work together closely in what is known as DevOps – a combination of development and operations (Bang et al. 2013) – by such means as continuous deployment and automated testing.

According to Spinellis (2012), DevOps is particularly applicable to SaaS products or to customized applications such as SAP ERP. A major DevOps enabler is an IT-system configuration management tool (ibid, p.2). These tools, available on a range of operating systems and architectures, take a model of a system's configuration. A model is stored in a repository in the form of a script. The tools translate models to device and operating system specific configurations (Delaet et al. 2010). A configuration management agent configures the device accordingly. Popular open source tools include CFEngine (2016), Puppet (2016), Amazon OpsWorks (2016), and Chef (Hintsch et al. 2015). Such tools allow cloud consumers to control and automate the configuration of all elements comprising an IT system: i.e. hosts, installed software, users, configuration files, scheduled tasks, networking, storage, monitoring, and security (Delaet et al. 2010). However, the current DevOps approach is limited to the usage of proprietary configuration tools focused on automation of operations (Bang et al. 2013). Nonetheless, one can use such open source configuration management tools to set up a new system starting from a blank slate, to add functionality to an existing system, and even to repair a system whose configuration is no longer up to date (or specification). In all cases, through the specification, you end up having at hand precise executable documentation of the system's configuration. This, according to Philip Armour's view of software as executable knowledge, makes IT-system configuration management not only an essential tool for developers but also an important craft and vital skill (Spinellis, 2012). While DevOps can work wonders when the organisation provides software as a service (like Google) or as a customized application (like the SAP ERP), these open source configuration management tools allow the configuration of SaaS and PaaS offerings. An exemplary research study in this field aims at the direct integration of lower-level configuration models with high-level service models, at making the service runtime environment transparent for service model users, and at achieving portability of service models between cloud providers (Wettinger et al. 2013). A popular example of Software as a Service is the customer relationship management offering by Salesforce.com. SaaS and PaaS can be provisioned on IaaS platforms. Different public IaaS offerings such as Amazon's EC2 or Rackspace exist. While Amazon uses its own software, RackSpace advertises its usage of OpenStack (RackSpace, 2016). OpenStack is described by Forrester's analysts (Forrester Research, 2016) as the new de facto model, which is also

used in academia (Leon et al. 2014). OpenStack may be deployed in a private, public, or hybrid cloud setting (OpenStack Foundation, 2016) and it can manage computing resources offered by virtualization hypervisors, para-virtualized containers, or bare metal nodes. Being that the setup, interconnectability, and configuration of a cloud SaaS application is a serious matter as it increasingly affects developers and users mainly due to the proliferation and complexity of various cloud-based offerings from different providers. Fortunately, this complexity can be controlled and conquered by adopting standards-based or open source IT system configuration management tools.

2.6 Enterprise Architecture Principles

At present, application development for cloud deployments follow two main approaches: (1) composition and (2) use of SaaS instances. Cloud applications are developed over the middleware offered through PaaS providers such as (Salesforce CRM, Google Apps etc.), or at a lower level of abstraction over IaaS providers, such as Amazon EC2, Microsoft Azure etc. (Baryannis et al. 2013). Enterprises run many applications to support their day-to-day business processes and operations. Such applications are implemented using a multi-tier architecture, which consists of a front-end tier, the business-logic tier, and a back-end tier. The flow of requests (or data) between these application components is often complex. A cloud application component typically comprises a set of operations with shared process, semantic, and access control. End users or other components of a cloud application service invoke multiple operations in certain ways to obtain results based on specific user roles with different access rights to operations performed and information obtained. The enterprise cloud application could be accessed by two types of users: (i) users internal to the enterprise; and (ii) users external to the enterprise (Hajjat et al. 2010). While a 3-tiered design is, the conventional architecture used in most applications, in practice applications are much more complex. For instance, each of these tiers may have multiple functional components, each component may have multiple functional servers performing the same role and executing the same code while load-balancers are employed to spread the requests across each server. With so many options for servers, hypervisors, storage and networking devices from various cloud providers, the degree of interoperability of an application can be measured as its cost of integration. Thus, it is imperative that cloud service developers (or creators) and architects design with a specific application in mind to ensure the infrastructure meets the scalability, reliability, interoperability and portability requirements of the application. Towards achieving this goal, there is a reason to standardise the interfaces to some cloud-based applications to permit collaboration industry sectors and application domains. To take advantage of cloud services, an enterprise needs an architecture based on loosely-couple services, not on information silo applications with tightly-coupled components (Open Group, 2013).

Per (Citrix, 2012), two distinct types of application workloads that have emerged in the cloud environment are: (a) traditional enterprise application; and (b) cloud-native applications. Most

enterprise applications fall into the former category (i.e. traditional applications). This includes applications developed by enterprise vendors such as Microsoft, Oracle and SAP. These applications are typically built to run on a cluster of front-end and application server nodes backed by a database. Traditional applications rely on technologies such as enterprise middleware clusters and vertically-scaled databases. The latter refers to a new style of application architecture that does not rely on enterprise-grade server clusters, but on many loosely–coupled computing and storage nodes. Applications developed this way often utilise technologies such as MySQL sharding, no-SQL, and geographic load balancing. A concise summary of basic architectural patterns for cloud applications is provided below. This is further substantiated with core application design principles that will reduce the cost of application integration for cloud computing and assist the development of an enterprise architecture that use and reap the full benefits of cloud services.

I. *Composite Application Architecture:* In a cloud environment, an application is composed of multiple independent components, each providing a certain set of functions. The application functions are scaled-out individually and are often offered by different providers. These components are integrated to form the functionality that the composed application offers. Often, a special language used for the composition of application component, in this context, is the Business Process Execution Language (BPEL) (Weerawarana et al. 2005). Due to this design the application is extendable right from the beginning and the integration of other applications is simplified (Fehling, 2011). Varia (2008) generally motivates why applications should be split into separate components when using cloud computing.

II. *Loose Coupling Application Architecture:* Cloud application components should be loosely coupled with the application components that interact with them. In a componentized application, management processes, such as scaling, failure handling, or update management can be simplified significantly, because components are treated individually. This however demands that the dependencies among components are reduced, so the addition, removal, failure, or update on one component has minimal or no impact on other components. This can be achieved by decoupling the components to reduce the assumptions one component makes about another one when they exchange information. In other words, the fewer assumptions two communication partners' make about each other, the looser they are coupled and the more robust are the functionality they provide. An application component should as far as possible be self-contained, with functions that are logically separate from those of other components. Interactions with other components within the application architecture should be simple, few, and not time-critical. Loose coupling comes at the price of performance reduction, since the communication path is longer as it includes address resolution and format transformation. Therefore, when designing an application, it generally should be weighted between loose coupling and performance.

III. *Service Orientation:* Cloud applications should be service-oriented. Service orientation is a way of thinking in terms of services and service-based development and the outcomes of services (SOA, 2014). A cloud application can be organised as a service, or a set of services, that may be a user of other services. Cloud computing services are normally exposed as Web services, which follow the industry standards such as Web Service Description Language (WSDL, 2016), Simple Object Access Protocol (SOAP, 2016) and Oasis Universal Description, Discovery and Integration (UDDI, 2016). The services organisation and orchestration inside clouds could be managed in a Service Oriented Architecture (SOA). A set of Cloud services furthermore could be used in a SOA application environment, thus making them available on various distributed platforms and could be further accessed across the Internet.

IV. *Stateless Application Architecture:* When a componentised application is distributed among several compute nodes, the chance that a failure occurs is increased. If the application is scaled-out, component instances are also added and removed regularly when the demand changes. To minimise failure, components should be implemented in a way that they do not contain any internal state, but completely rely on persistent storage. However, since the component instances do not have an internal state, no data is lost if an instance fails. Such a setup significantly increases the capability of the componentised application to scale-out, because multiple components can share a common data store and thus act as if they had the same common internal state.

Regardless of the significant impact of cloud computing on enterprise architectures for organisations of different sizes and customers, still organisations are formulating schemes and roadmaps for migration to cloud computing environment. However, for companies to adopt cloud computing in a way that aligns with their business strategy, enterprise architecture (EA) is an absolute necessity. Enterprise architecture characterizes and models the enterprise through a set of interrelated layers or views: strategy, business, data, applications, and technology (Aureli, 2012). This insight helps stakeholders to design, assess, and communicate the consequences of decisions and changes within and between these business domains. Enterprise architects, responsible for drawing and deciding about open and extensible EAs, need to relook their current architectures and ponder about viable means and mechanisms to incorporate the emerging and evolving cloud aspects into their architectures (Raj and Periasamy, 2011). Therefore, a company which decides to shift into the cloud must have a mature and well-formed understanding of the EA on which is based and, thus, a clear view of components which concern it. This understanding is necessary for the enterprise to make meaningful decisions related to cloud computing. In addition, the organisation will have well defined interoperability guidelines. As stipulated by (Raj, 2013), below are the core architectural principles for organisations to consider and adhere to when designing a successful cloud application solution for use in any enterprise:

- Stable interfaces – cloud application components should have interfaces that do not rapidly change over time, or are such that any changes made are backwards-compatible with earlier formats/interface. The lifetime cost of a cloud application component whose interfaces is unstable will be considerably more than its initial cost of integration. It is recommended that the cost of integration of a cloud application component be considered over its lifetime, not just at its point of first use. Moreover, the interfaces to cloud application components should be clearly described in either machine-readable and/or human-readable descriptions.

- Secure – guaranteeing delivery of agreed-upon security levels (e.g., threat protection, privacy, and compliance), data and intellectual property protection. Considerations for Identity, Entitlement, and Access Management (IEM) and/or Role-Based Access Control (RBAC) for the enterprise Cloud Ecosystem.

- Seamless – combining public and private cloud services with traditionally deployed services and outsourced services to deliver a seamless experience. This also includes seamless collaboration and integration capabilities with partners, suppliers, and back-office.

    - Portability and interoperability should be considered to ensure disparate services, perhaps provided by multiple cloud service Providers, can seamlessly interact.

- Resilient – providing sure delivery of agreed-upon availability, quality, and performance service levels.

- Automated – incorporating policy-based automation and management that integrates cloud with legacy assets and services to provide integrated service catalogues and end-to-end service quality.

- Open, not locked-in – comprising modular infrastructure and services that support heterogeneous environments. Additionally, the enterprise must adopt an IT strategy that not only builds internal clouds but also utilizes external clouds to enhance business agility and support.

2.6.1 Approaches for Enabling Cloud Portability and Interoperability

Portability and interoperability combine to provide compatibility of cloud solutions. They are important considerations for cloud planning because together they ensure that cloud solutions continue to operate (through interoperability) and do so unchanged (through portability). When portability and interoperability between components is not addressed, unanticipated processing failures will be the likely result with the associated costly disruption of business continuity. The

following are existing approaches for enabling portability and interoperability in the cloud computing environment.

1) **Model-Driven Approach (MDA)**

The Object Management Group (OMG) MDA architecture for Design, provisioning, execution, or migration to the Cloud, is a model-based approach for the development of software systems that aims at separating the platform-independent design of a software application from its implementation on a given platform. From the cloud perspective, the main feature and benefits of MDA are the enablement of portability, interoperability, and reusability of (parts of) the system, as well as its easy maintenance, through human-readable and reusable specifications at various levels of abstraction (Martino et al. 2015). Model-driven development in the context of cloud computing, allows developers and enterprise architects to design software systems in a cloud-agnostic manner. This approach which is often summarized as "Write Once, Run Anywhere" or WORA, and is particularly relevant in designing and managing applications across multiple clouds, as well as migrating them from one cloud to another. Combining MDA in the cloud computing domain is currently the focus of several research groups and projects, such as MODAClouds (Nitto et al. 2013), ARTIST (Menychtas et al. 2013) and REMICS (Mohaghehi et al. 2010).

2) **Semantic Approaches**

As pointed out earlier in section 1, one of the contributory factors of interoperability and portability problems in the cloud environment is the differences in the semantics of resources offered, since no uniform representation exists. As stated by (Sheth and Ranabahu, 2010), semantic models are helpful in three aspects of cloud computing:

1. Functional and non-functional definitions refer to the ability to define application functionalities and quality-of-service details in a platform-agnostic manner

2. Data modelling, including meta-data added through annotations pointing to generic operational models, which plays a key role in consolidating API's descriptions

3. Service description enhancement, in particular regarding service interfaces that differ between vendors even if the operations' semantics are similar.

Existing technologies inherited from the semantic web field can be useful to address these aspects above. In particular Web Ontology Language (OWL) (Aversa et al. 2012), OWL for Services (OWL-S) (Mark et al. 2004), SPARQL RDF Query Language (Prudhommeaux et al. 2008) and Semantic Web Rule Language (SWRL) (Horrocks et al. 2004).

3) **Multi-Agent Systems (MAS)**

MAS can be defined as a computerised system composed of interacting intelligent agents, collaborating within the same environment. An agent is an autonomous entity, represented by a software program. According to (Talia, 2011), agent-based solutions can improve cloud resources and service management and discovery, SLA negotiation, and service composition. MAS offers effective approaches to solve a number of interoperability issues and automate a number of activities, in particular brokering, negotiation, management, monitoring, and reconfiguration in multiple clouds (Martino et al. 2015).

4) **Cloud Patterns**

Cloud computing patterns are logical descriptions of the physical and virtual assets that comprise a cloud computing solution (Iannucci et al. 2013). Cloud patterns arise from the need to provide both general and specific solutions to recurring problems in the definition of the architectures for cloud applications. While classical design patterns deal with problems related to different aspects of software development, cloud patterns mainly focus on the architecture of the cloud application. Consequently, this has led to the development of platform-dependent patterns, which can be applied only to a specific platform offered by a specific vendor. Despite the poor flexibility of some vendor-specific patterns, cloud patterns still represent a valuable means to enhance portability and interoperability between cloud platforms. Patterns can be used to describe and model existing cloud applications in a very easily understandable manner, tracing back cloud implementations to a set of well-known and stable solutions. In this way, it becomes easier to understand the exact functionalities and responsibilities of a specific cloud application component, which can later be substituted with a compliant one having the same or similar characteristics. This approach can be exploited also in the case of porting non-cloud applications (i.e. traditional enterprise applications), describable through classic design patterns, to a cloud environment, provided a mapping between design and cloud patterns' participants exists (Martino et al. 2015).

5) **Cross-Platform API**

Cloud APIs specify how software applications interact with a cloud-based platform where these applications can be deployed. According to Petcu and Craciun (2011), cross-platform APIs for cloud computing are emerging due to the need of the application developer to combine the features exposed by different cloud providers and to port the codes from one provider environment to another. Such APIS are allowing the federation of clouds to an infrastructure level, requiring certain knowledge of programming the infrastructure. It is expected nowadays that using a cross-platform API the developer of an application calls a common unified API and get a standard based answer regardless of the implementations of different providers.

Although cross-platform APIs were produced initially for infrastructure provisioning models, however, herein author mentions the recent proposals by standardization groups, like OCCI and UCI. For instance, Opensource solutions like libcloud, jClouds, SimpleAPI or OpenNebula, and commercial ones, like DeltaCloud are designed either to interface only with Java, Python or PHP, or they are providing connectors or wrappers to a small number of cloud provider offers. For this reason, it is considered that in order to eliminate the vendor- lock in problem caused by interoperability and concerns (or lack thereof), a new approach for a cross-platform API is needed with a common set of interfaces for all provisioning levels (i.e. service, application and infrastructure). Such API should not only be platform independent but also language independent.

2.6.2 Implications of Integration and Interoperability for Enterprise Applications

A short overview of enterprise system and application integration is beneficial to understanding the current views of cloud integration, and interoperability requirements. In the past, enterprise application and data were linked within corporate intranet through one or more standards-compliant integration platforms, brokers, and backbones such as Enterprise Architecture Integration (EAI), Enterprise Service Bus (ESB), and Enterprise Information Integration (EII). Over the past few decades, there has been an evolution in integration architecture across the industry, with progressively greater degrees of API exposure for a business function as depicted in **Figure 2.11**.

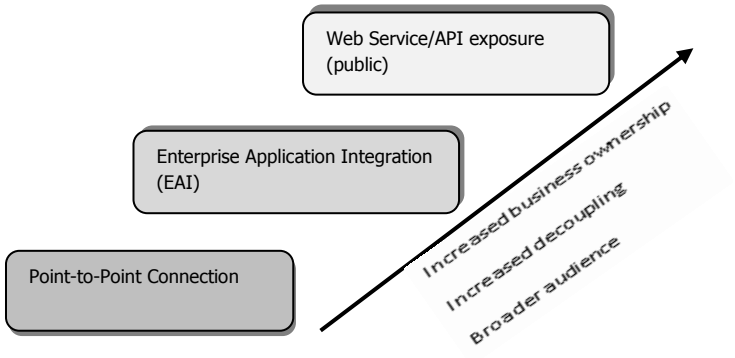


Figure 2.11-Progressive exposure of enterprise integration architectures (Adapted and modified from [Clark, 2015])

As enterprises continuously strive to reduce business complexity and improve user productivity through process standardization, the ease with which cloud solutions can be deployed holds obvious appeal (Ebneter et al. 2010). For many enterprise businesses, cloud computing is an attractive deployment option. There are several reasons for this; the scalability, multitenancy, elasticity and on-demand access of the cloud etc. removes many barriers to enterprise deployment. While cloud applications offer outstanding value in terms of multitenant features and functionalities,

they introduce several integration and interoperability challenges that hinder enterprises' decisions for or against cloud adoption and migration. The first challenge is that, many organisations have different systems and applications that consist of numerous technologies, protocols, applications and devices distributed across a network (Mahmood and Hill, 2011; IBM, 2012). In such heterogeneous environments, information can come from many places — such as transactions, operational, document repositories and external information sources — and in many formats, including data, content and streaming information (Tolk, 2013). In this aspect, lost, inaccurate or incomplete information also can generate high costs and lost productivity when having to search for information or synchronize data. Moreover, poor data quality can lead to failed business processes and erroneous decision-making. The second challenge is that most core enterprise applications (such as Customer Relationship Management or CRM, Supply Chain Management or SCM and Enterprise Resource Planning or ERP systems) are being packaged to the cloud in a Software-as-a-Service (SaaS) model, and delivered to companies as point solutions that service only one line of business (LoB). As a result, organisations without a means of synchronizing data between multiple LoB are at a serious disadvantage in terms of maintaining accurate data, inability to make real-time and information-backed decisions, and difficulty in realizing complete business process automation. Real-time sharing of data and functionality becomes difficult in such distributed computing environment. Finally, considering each vendor that provides a cloud solution creates its own interface to the application. This fact creates a challenge in organisations of all sizes (small or large) and locations as they attempt to understand and then manage these unique application interfaces, and integrate applications from cloud to cloud and cloud to on-premise systems.

Therefore, as enterprise environments are becoming increasingly distributed and heterogeneous, there is a need to integrate between disparate systems to satisfy certain business requirements and needs. In this paper, we argue that interoperability is one of how enterprises can achieve such integration. Interoperability, which is the ability to exchange data between two or more systems by adhering to common standards, contends with the software and implementation details for interoperations. This includes exchange of data via interface standards, the use of middleware, mapping to common information exchange models etc. (Joshi et al. 2014). Integration on the contrary deals with the technical connections between systems. Without agreed upon standards shared by at least two systems, enabling seamless interaction between business processes in a heterogeneous environment becomes a challenging task. Since integration and interoperability both build upon standards, standardization should be considered as the key to achieve integration and interoperability in a distributed cloud environment.

2.6.3 Essential Features of Cloud Services Interoperability and Portability

Cloud computing consumers do not have direct visibility into the physical computing resources; instead they interact with service providers through various service model interfaces to gain a view of the abstracted computing resource they are using. As it would be expected, there are a broad range of capabilities and functions available in the various cloud provider interfaces currently available. While standardisation of cloud interfaces is maturing, commonalities among provider interfaces can help cloud customers understand the key interoperability and portability requirements and features. Figure 11 shows the three main interfaces between a cloud service customer (system user-roles) and the cloud service. These interfaces presented to cloud consumers are broken down into three categories (i.e. functional, self-service administrative API, and business interfaces), with interoperability and portability determined separately for each category. For instance, in **Figure 2.12**, each type of cloud service offering (IaaS, PaaS, and SaaS) presents an interface for each category. The functional interfaces are associated with the main functional capabilities offered by the cloud services. Whereas, the business interface involves capabilities relating to the business aspects of the cloud service that includes subscription information, billing and invoicing. The administrative self-service management API involve interface capabilities for administering the cloud service and includes capabilities such as monitoring the service and managing its behaviour. This also includes aspects of security such as user identities, authentication tokens and authorisations. In a cloud service environment, APIs are typically defined by a programmatic interface based on common protocol such as REST/JSON or SOAP. Notice, the interface that is presented to (or by) the contents of the cloud service encompasses the primary function of the cloud service. This is distinct from the interface that is used to manage the use of the cloud service.

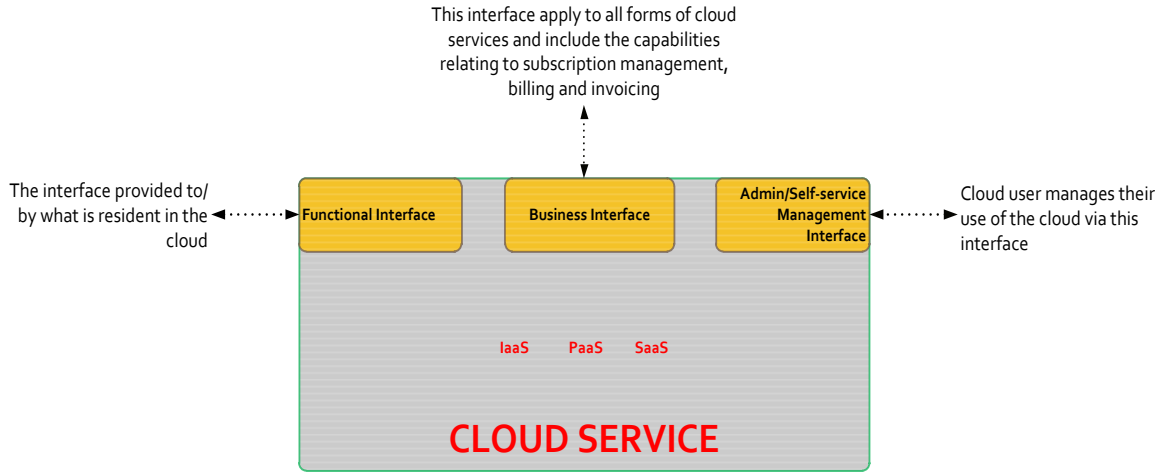


Figure 2.12-Cloud Service Interface Category

Service Model-specific Interface Capabilities and Standardisation Opportunities

It is important to understand that each of these interfaces described above, may have multiple forms. For instance, the main capabilities of a cloud software application may be presented in the functional interfaces to end users as a web browser application or as a mobile App. Moreover, the same capabilities may also be made available as an API for consumption by custom applications written or purchased by the customer and running on the customer's system. As an example, using the illustration in the diagram below (see **Figure 2.13**), the functional interface of an IaaS cloud offering is a virtualised Central Processing Unit (CPU), memory and Input/output (I/O) space used by an OS (and the stack of software running in that OS instance). In other words, the functional interface for an IaaS cloud is tied to the architecture of the CPU that is being virtualised. This not a cloud-specific interface as de facto CPU architectures are the norm, thus no effort is being put into a de jure standard for this interface. Whereas, the cloud service user utilizes the management interface to control their use of the cloud system by starting, stopping, and manipulating virtual machine images and associated resources. The self-service IaaS management interface, however, is a candidate for interoperability standardisation, and there are several efforts in this space: The Open Cloud Computing Interface (OCCI) from the Open Grid Forum (OGF) and Cloud Data Management Interface (CDMI) standard are examples of both storage management interface as well as a storage functional interface for IaaS resource management interface.

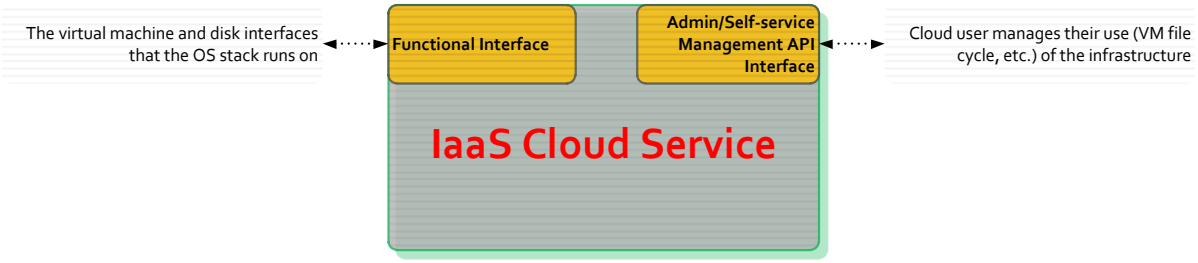


Figure 2.13- IaaS Interface capabilities for Interoperability and Portability

For PaaS, the functional interface is a runtime environment with a set of libraries and components for developers to develop and deploy SaaS applications (see **Figure 2.14**). This could be offered in different languages and may or may not take advantage of existing application platforms standards such as those found in J2EE or.Net environments. However, the management interface of a PaaS offering as depicted in the figure below is very like the management interface of an IaaS offering. In this case, instead of the virtual machine and resources, the management API is concerned with the lifecycle of the applications and platform resources they depend on. Moreover, instead of being metered and billed based on virtual hardware resources, the business interface typically exposes metrics for platform service and runtime container usage (e.g. Docker). Interoperability of PaaS self-service management interfaces can be achieved separately from the interoperability of the PaaS

functional interfaces, although there seem to be very few efforts concentrating on PaaS management interfaces today. For example, standard-based APIs are often part of a PaaS offering such that the PaaS provider can enable existing development for a cloud-based hosting system. However, data format for backup and migration of application workload, including database serialization/de-serialization, need further standardization to support portability (Pritzker and Gallagher, 2013).

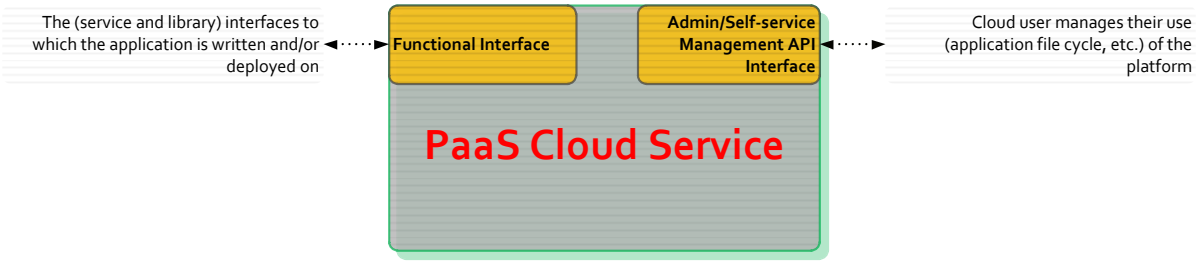


Figure 2.14-PaaS Interface capabilities for Interoperability and Portability

In Figure 2.15, the functional interface of a SaaS cloud offering is the same as the application interface of the software itself. The varieties of the SaaS applications determine what can be consumed by the SaaS consumer. For instance, where a SaaS application is consumed through a Web browser, there may be many standards used to achieve interoperability between the Web server and user's browser, such as IP (v4, v6), TCP, HTTP, SSL/TLS, HTML, XML, REST, and JavaScript/JSON. None of these Web standards are cloud-specific since they are being used across many Web browser-based management interfaces. However, in the case where the SaaS application is consumed by another system as a service (e.g. composition-as-a-service model), cloud or otherwise, there are various standards as to both data content and interfaces. A potential area for standardisation is the metadata format and APIs to describe and generate e-discovery metadata for emails. Most important for interoperability are canonical data content formats, commonly expresses using XML standards. The self-service administrative management interface of a SaaS offering is concerned (not with the life cycle but) with the administration and customization of application functionality for each user of the offering. For example, through this interface additional users can be added (along with other credentials and permissions), additional features can be ordered for each user (or tenant), and an accounting of each user's (or tenants) consumption of the offering is available. Due to the diverse domain and functional differences among SaaS offerings, the management interfaces used for the consumers to administer and customize the application functionalities are also very diverse. However, certain management functionalities are common, such as those related to user account and credential management. These common management functionalities represent candidates for interoperability standardisation.

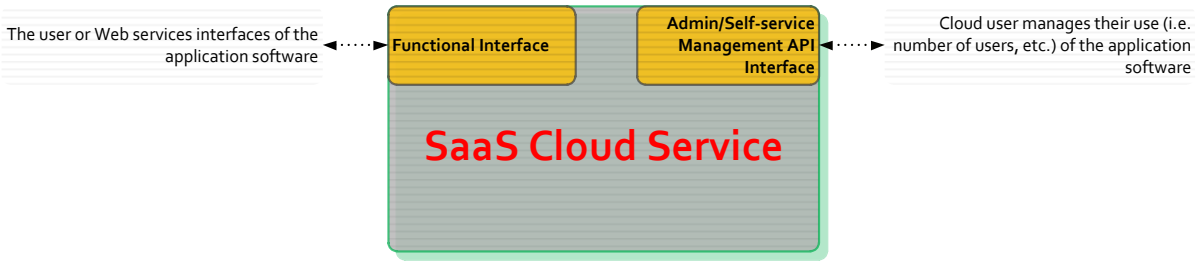


Figure 2.15-SaaS Interface capabilities for Interoperability and Portability

Cloud Computing (SaaS) Interoperability and Portability Scenarios/Considerations

Understanding the interoperability and portability features of cloud services is a requisite step for planning and designing for the effective use of any cloud service. Due to the high number of variable that come into play in a complex cloud computing solution that involves interoperability and portability capabilities – several use cases have been defined to underline the requirements and consideration of the case. Among the several cloud-computing use case scenarios, we report and classify some notable example(s) in current literature to highlight the key aspects of cloud computing interoperability and portability. The result of the classification is illustrated in **Figure 2.16**, where broken lines represent nature of interaction (via a prescribed API) between cloud service consumer and provider components.

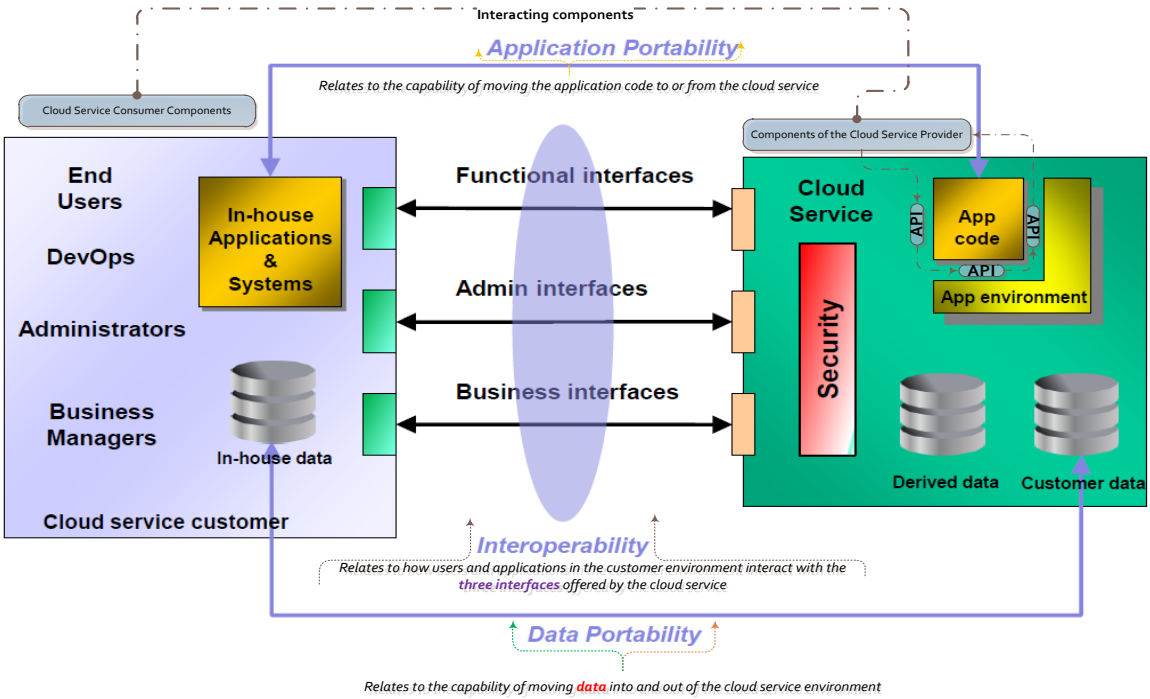


Figure 2.16-Essential features of Cloud Service Interoperability and Portability [Adapted and modified from (CSA, 2014)]

In **Figure 2.16**, the application (App) code within the cloud service can be taken to represent the customer application code in case of IaaS and PaaS cloud services, but in the case of a SaaS service, the application code would typically belong to the provider and would be managed by the provider. The application environment represents the API that the cloud service presents to the application code; and the application code should be able to use this API for the application to run. In this case, the App environment could be the operating system, or it might be an API offered by some middleware framework, depending on the nature of the cloud service. The security component represents a set of capabilities which are used to secure the cloud service and includes authentication and authorisation of users, encryption of data in motion and at rest, firewalls and technologies for dealing with attacks such as distributed denial of service (DDoS) etc. Data which are associated with the cloud service are classified as; cloud service customer data, cloud service provider data (is omitted from **Figure** above), and cloud service derived data. As illustrated in **Figure 2.16**, cloud service customer data is a class of data objects under the control of the cloud service customer. It includes data input into the cloud service by the customer; such data may be held as records in a database or as data objects in files or in a data store. Cloud service provider data (omitted from diagram) is a class of data objects, specific to the operation of the cloud service, under the control of the cloud service provider. Cloud service provider data includes but is not limited to resource configuration and utilization information, cloud service specific virtual machine, storage and network resource allocations, overall data centre configuration and utilization, physical and virtual resource failure rates, operational costs etc. Cloud service derived data represents data which is created and stored because of the cloud service customer use of the service (such as log records or configuration information), the intended uses for derived data and what rights the cloud service customer has to inspect the derived data.

One of the key elements to interoperability and portability is data portability. While the systems interoperability becomes the primary concern of the cloud service provider, issues around data interoperability and portability remains critical. Often, the onus is on the cloud consumer to ensure that the data is portable as the consumer owns the data. Therefore, it should be mandatory for all cloud customers to acknowledge that in substituting cloud providers, data must be in a format that is sharable between the cloud providers, since without ability to port data it will become impossible to switch providers. To achieve a fully interoperable cloud computing services, you need to achieve three levels of interoperability:

1. Technical Interoperability – Bits and bytes are exchanged in an unambiguous manner via a set of standardised communication protocols

2. Syntactic Interoperability – A common data format is defined for the unambiguous sharing of information

3. Semantic Interoperability – The meaning of data is exchanged through a common information model and the meaning of information is unambiguously defined and shared

Note, semantic interoperability is not common practice today; it is this focus on the data semantics that will facilitate the drive towards interoperability. However even if you enable all these capabilities there is one more key step required which is to delegate the syntactic and semantic interoperability to a software infrastructure layer (common across every sub-system). The means of associating interoperability with data and information flows at the system level is to use a data-centric design approach.

2.6.4 Differences between Interoperability, Portability, Integration and Compatibility

The objective here is to provide an explanation of the four terms as used interchangeably in the cloud computing terminology. Unfortunately, the four terms are often conflated in the existing literature. So, the rationale for providing the following explanations is, because when things that are different are grouped together and treated as things that are similar, error is assured. Therefore, to avoid such error(s) as misrepresentation of facts, author provides the following definitions and distinctions to aid the readability and validity of this thesis. To explain the terms concisely, two basic entities are required: i.e. components and systems. Components are one of the parts that make up a system, while a system is a collection of components organised to accomplish a specific function or a set of functions.

1. **Interoperability**: The concept of interoperability as it applies to cloud computing is at its simplest, the requirements for the components of a processing system to work together to achieve their intended results. Interoperability checks that interactions with components that it is intended to support work correctly. So, interoperability is concerned with the ability of two or more systems or components to communicate, and it requires the communicated information can be understood by the receiving system. In other words, components should be replaceable by new or different components from different providers and continue to work. For example, typical components required of a cloud system include: hardware, operating system, virtualization, networks, storage, software (applications, frameworks, middleware, libraries etc.) and data security. With appropriate interoperability between components attained, companies can effectively deploy cloud solutions from a single cloud provider or from many providers as best meet their business needs. Interoperability is therefore involved with the interfaces (as with integration) but not with whether the communicating systems behave as specified. **Figure 2.17** below illustrates how two systems (1 and 2) communicating with an interface in each system to handle the communication. The interface provides the information for use by the receiving system at the point marked ‘A’.

Figure 2.17-Interoperability Testing

Note: Interoperability testing is limited to checking that information is correctly communicated from one system and arrives at the other system at the point marked 'A' in a useful state. I.e. interoperability testing is a subset of integration testing

2. **Portability**: Portability is concerned with the ease of moving components or systems between environments (hardware and/or software environments). The concept of portability as it applies to the cloud provides for application and data components to continue to work the same way when moved from one cloud environment to another without having to be changed. Portability of applications means that an application running on one cloud platform can be moved to a new platform and operate correctly without having to be re-designed, re-coded, or re-compiled. Whereas, portability of data means that databases, data files or other data elements used within application or user processing can be moved to any new environment and used without requiring changes to the data format or to the applications that use it. A portable component can be moved easily and reused regardless of the provider, platform, operating system, location, storage or other elements of the surrounding environment. In **Figure 2.18***(a)* components 'B' can be seen in two different environments (I and II), whereas in **Figure 2.18***(b)* system 'J' can be seen in two different environments (III and IV). In as much as components 'B' and system 'J' can work correctly in the different environments then they are portable components and systems.

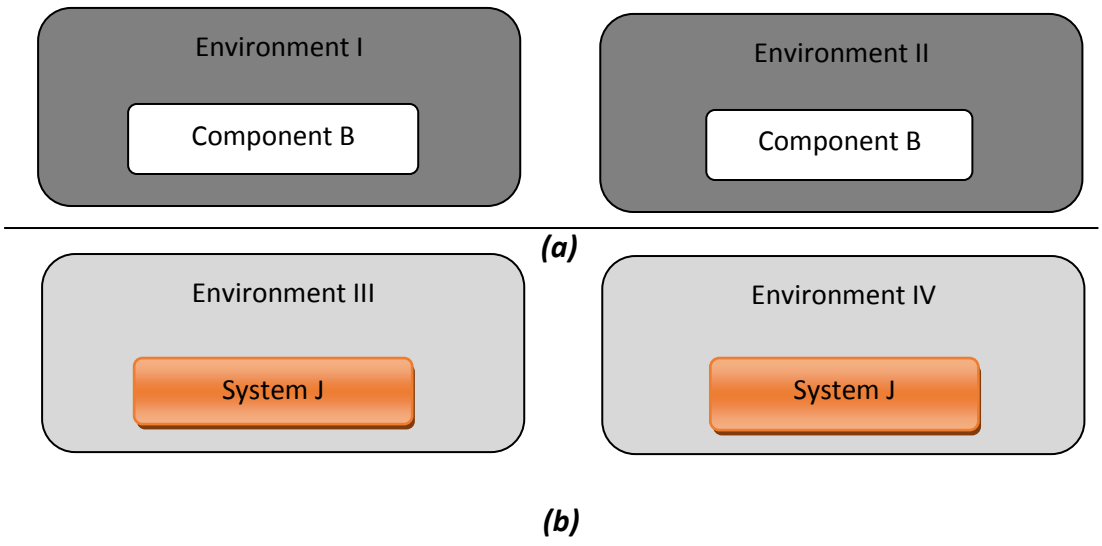


Figure 2.18-Portability Testing

3. **Integration:** Integration is concerned with the process of combining components into an overall system. In software design paradigm, integration is concerned at two levels. First is the integration of components at the module level into a system (often referred to as component integration). Second is the integration of systems into a larger system – sometimes known as system integration. Overall, integration is concerned with whether the interface between components is correctly implemented, but also with whether the integrated components (now as a system) behave as specified. This behaviour will cover both functional and non-functional aspects of the integrated system. **Figure 2.19** shows two components 'X' and 'Y' interacting to form an integrated system.

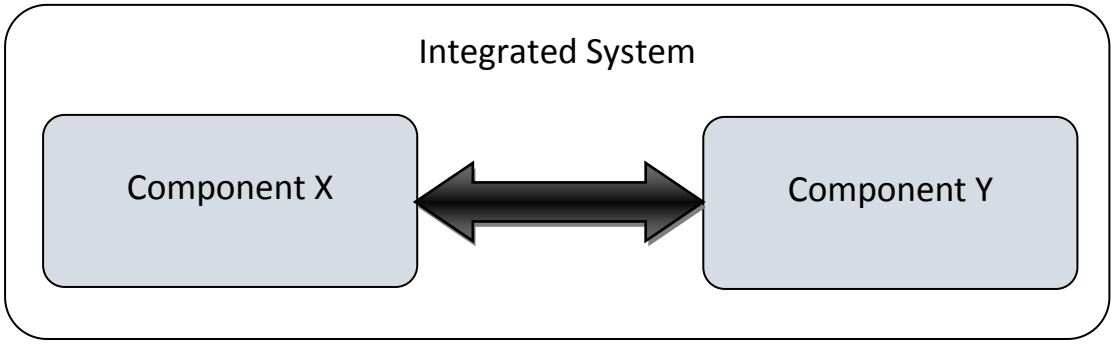


Figure 2.19-Integration Testing

Note: Integration testing is concerned with whether the two components when combined (i.e. integrated) to form an integrated system behaves as the system is expected to behave.

4. **Compatibility:** Compatibility is concerned with the ability of two or more systems or components to perform their required functions while sharing the same environment. The two components (or systems) do not need to communicate with each other, but simply be resident on the same environment. Compatibility checks for un-intended interactions that disrupt normal business process operation. So, compatibility is not concerned with interoperability since two components (or systems) can also be compatible but performs separate functions. In other words, compatibility is next natural step of how to achieve this interoperability. It is the ability of the application and the data to work the same way irrespective of the service model (i.e. IaaS, PaaS, SaaS) or deployment models (private, public, and hybrid) and location (internal or external to the enterprise). **Figure 2.20** shows two components in the same environment. They are compatible with each other if both can run (or simply reside) on the environment without adversely affecting the behaviour of the other.

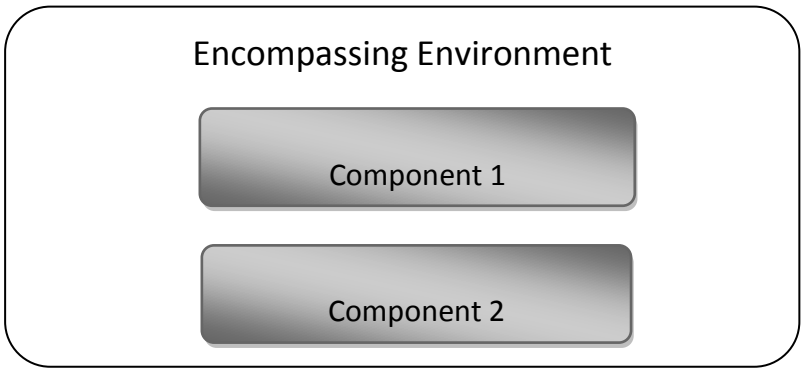


Figure 2.20-Compatibility Testing

2.7 Heterogeneous Cloud Computing Environments

Cloud computing is an evolving paradigm in the delivery and consumption of IT services, but its unique aspects exacerbates problems with vendor lock-in. The evolution has been a result of a shift in focus from an infrastructure that delivers storage and compute resources to one that is economy based aiming to deliver more abstract resources and services. This sub-section explores heterogeneity in cloud computing environments and describes the risks of vendor lock-in that are either caused or intensified by heterogeneity.

The issue of heterogeneity as it relates to cloud computing is that operating systems (OSs), hardware, software, virtualization, storage, data security, networks, and application components all interact to provide critical business functions. Combining these components from different CSP into a unified solution introduces boundaries (i.e. distinct divisions across which data and or apps. move or operate) between different components. Boundaries may exist between physical locations, across OSs or different platforms, service providers, or even between applications (or app. components) and between separate or distinct data stores. Ensuring operational integrity across these boundaries when data and application processing needs move into the cloud is a critical consideration that raises different issues related to integration, portability, and interoperability. These issues surface simply because cloud computing introduces new platform services and technology components, leading to technology architectures that are quite different from those that support traditional applications. Moreover, in the cloud computing ecosystem, the vast variety of cloud infrastructures with different OSs, platforms, and wireless network standards further is making cloud application development a major challenge for developers. As clearly pointed out by (Takabi and Joshi, 2010), heterogeneity in clouds comes in different forms. First, as pointed out above, cloud providers use various hardware and software resources to build cloud environments. To some extent, resource virtualization achieves high-level system homogeneity, but the same infrastructure being used to support different tenants with different protection and system requirements can generate difficulties. Secondly, there is also a potential issue with vertical heterogeneity of cloud services. For instance, a CSC might subscribe to

an IaaS from one provider, couple it with a PaaS from another cloud provider, and acquire various pieces of SaaS from a third cloud vendor. The assumptions that each of these cloud providers make in building the services can severely affect the emergent standards, trust, and security properties. Furthermore, heterogeneity exists in the level of security treatment each component provides, thus generating integration challenges. A major source of heterogeneity in cloud environments is physically different processor architectures. This can occur either when a mix of machines is purchased initially or when a data centre adds machines of a different type. Differences between processors directly affect performance, as newer generations typically incorporate more advanced pipelines and memory systems.

To deduce from the paragraph above, heterogeneity in cloud computing is simply the existence of differentiated hardware, architectures, infrastructure, and technology used by cloud providers. Many cloud vendors provide services based on custom-built policies, infrastructure, platforms, and APIs that make the overall cloud landscape heterogeneous. Such variations cause interoperability, portability, and integration challenges. Moreover, one essential characteristics of cloud computing is the ubiquitous network access, where ubiquity means that the cloud provider's capabilities are available over wide area network (WAN) and can be accessed through standard mechanisms by both thick and thin clients. But WAN environments are known to be heterogeneous medium of communication, because they consist of equipment from multiple vendors across multiple network domains. Possible variations at the network layer and related technologies of the cloud computing stack will impact the delivery of cloud services and affect mobility of services across different provider environments. Additionally, there is the notion that contemporary market dynamics raises business competition, which in turn also diversifies cloud providers with their heterogeneous frameworks, further exacerbating heterogeneity on cloud side. This heterogeneity creates complex challenges related to vendor lock-in. Also, managing security policies and SLA automatically in cloud infrastructure and platforms is more complex due to the heterogeneity among various entities. Hence, understanding heterogeneity roots in cloud computing can significantly enhance interoperability and portability of cloud services and avoid vendor lock-in. So far, our review of distributed cloud computing environment has shown that heterogeneity remarkably intensifies the risk of vendor lock-in, and thus necessitates an in-depth analysis. While this paper strives to explore heterogeneity in the cloud ecosystem, it also provides insights into essential dimensions of heterogeneity that could intensify the vendor lock-in problem. In the next section, we present taxonomy of heterogeneity roots in cloud computing, with the hope to paint a clear picture of how vendor lock-in is created, intensified by non-compatible underlying technologies, and what kind of challenges cloud services can face, due to lack of interoperability and portability, as they gain adoption in enterprises.

2.7.1 Heterogeneity Dimensions in Cloud Computing

Analysing the roots of heterogeneity in cloud systems has shown significant differentiation in silo of cloud and communication networks. The proposed taxonomy depicted later in *Figure 2.22* shows how nine underlying cloud computing components are influenced by heterogeneity. However, further analysis and scrutiny of this taxonomy confirms that heterogeneity in distributed cloud computing environments is two-dimensional; i.e. horizontal and vertical, as illustrated in **Figure 2.21**. Thus, in this section, we briefly describe heterogeneity dimensions in cloud computing and its impact in exacerbating the problems of vendor lock-in.

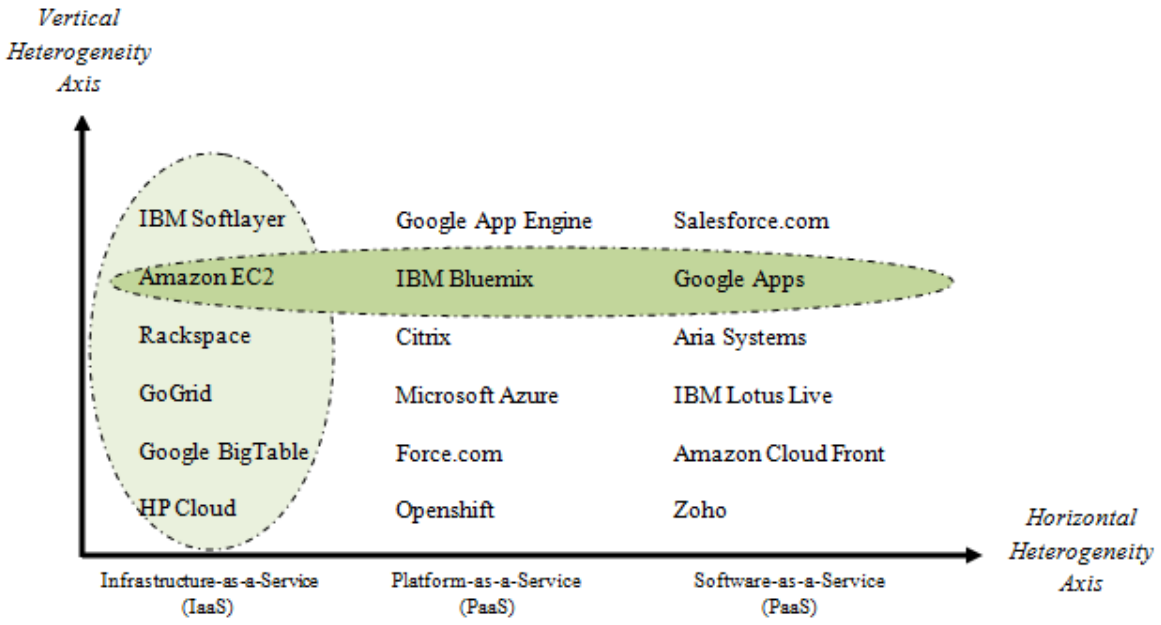


Figure 2.21-Heterogeneity Dimensions in Cloud Computing

- ***Vertical Heterogeneity***: When differentiation is within a single type of OS, cloud service, or wireless network it is named vertical heterogeneity. In the cloud, vertical heterogeneity occurs within a single type of clouds that provides similar services, e.g. IaaS (Infrastructure as a Service) or PaaS (Platform as a Service). The vertical oval shape in **Figure 2.21** shows vertical heterogeneity within various IaaS service vendors. Though Amazon EC2 and Rackspace are IaaS clouds, they are built on different pillars: internal infrastructures, technologies, and business policies. Therefore, demand for switching between these two cloud services incurs redundant cost, even though both vendors provide IaaS. It also creates data and application portability issues and hinders easy code and data migration within a single type of clouds. In turn, cloud users are forced to adhere to specific cloud service provider(s). However, standardization efforts like the

Open Virtualization Format (OVF), TOSCA, and CAMP are emerging to alleviate problems and facilitate the deployment of virtual appliances in various clouds.

- ***Horizontal Heterogeneity***: When differentiation is across different types of mobile OSs, cloud services, or wireless networks it is named horizontal heterogeneity. In the cloud, horizontal heterogeneity occurs between different types of clouds that provide heterogeneous services, like IaaS and PaaS. The horizontal oval shape in **Figure 2.21** shows horizontal heterogeneity between various types of cloud services. In a scenario that some PaaS vendors offer free limited storage, if a new application utilizes such storage that is incidentally coupled with specific data structure like Google App Engine (the only GQL-based PaaS cloud), such dependency locks the application in the cloud. Hence, porting rapidly growing data to an IaaS cloud (for less hosting cost) which is non-GQL-based IaaS (e.g. SQL-based cloud) is hardly possible and inflicts upfront investment. This type of heterogeneity is more difficult to address as compared with vertical heterogeneity because of switching difficulties between various service providers with different patterns, architectures, APIs, and business policies.

2.7.2 Taxonomy of Heterogeneity Roots in Cloud Computing Services Infrastructure

Due to the vital influence of heterogeneity in creating or intensifying cloud lock-in, we comprehensively examine the dimensions of heterogeneity in cloud computing environments. In this vein, we identify heterogeneity roots in cloud computing as; hardware, operating systems, virtualization, networks, storage, software (application frameworks, middleware, libraries, and applications), features, data security and API. When put together, these components are typically required to build and maintain a cloud system. Thus, they are extremely important to understand the main lock-in challenges that clouds face today, and should overcome in the future. Therefore, with help of these components, as shown in **Figure 2.22**, we devise a taxonomy of heterogeneity roots in cloud computing, and offer recommendation and considerations as it relates to portability and interoperability when moving data and applications securely to and from the cloud. The criterion for defining the taxonomy is deeply rooted on the core ideas of distributed systems, but with a focus on cloud architecture, services, virtualization management etc. We hope this taxonomy will help many discerning readers, developers, enterprise architects, and researchers in the cloud community gain deeper understanding of heterogeneity roots in the cloud, and provide a more detailed analysis of the risk of vendor lock-in to the general audience. We provide comprehensive details of the aforesaid in the subsequent sections.

2.7.2.1 ***Hardware Heterogeneity:*** Hardware components will inevitably vary from one provider to another leaving an unavoidable interoperability gaps if/when direct hardware access is required. Variety of hardware with different architecture between cloud servers, storage,

and network infrastructures trigger hardware heterogeneity in the cloud that could give rise to a vendor lock-in situation. In the cloud environment, cloud providers maintain different infrastructures and architectural design to enhance quality of their service. Servers for instance, use X86 Complex Instruction Set Computer (CISC) architecture with two variations of 32-bit and 64-bit. Moreover, cloud infrastructures gradually grow more heterogeneous due to upgrade and replacement. The emerging growth of cloud computing will increase the number of geographically distributed cloud nodes that intensifies hardware heterogeneity among cloud providers. Thus, the question is how to ensure geographically diverse components work together? Nevertheless, hardware and architectural heterogeneity among cloud components hamper direct deployment of cloud resources and services and raises more challenges as listed and briefly discussed below.

- Information System Architecture and Data management: Heterogeneity in the cloud ecosystem brings new dimension to data architecture, by introducing cloud data storage services (NoSQL), and by facilitating processing of big data. The increasing number of very large scale geographically distributed data centres and the non-similarity of data structures complicate data management. Integrating huge distributed data and providing virtually unified storage for cloud consumers is becoming more complicated with the ever-increasing heterogeneity in cloud services.

- Data Interoperability: Data interoperation is the ability of connecting heterogeneous networks, understanding geographical information resources, and exchanging data between/across two or more heterogeneous systems. However, the infrastructure diversity among various clouds on one hand and dissimilarities between them and with existence of various network hardware systems on the other hand, have created data integration and interoperation problems in the absence of interface standards and uniform platforms. The data interoperation problem is to guarantee that all components of the cloud system share the same understanding of the data transmitted, where the same understanding means that they have consistent semantic representations of the data (Blair et al. 2011).

- Portability: Codes are not easily movable and executable to/on heterogeneous hosts and the privilege of “Write once run anywhere” or WORA is divested from developers. For instance, the application written for quad-core processor is not executable on dual-core processor due to architectural and hardware dissimilarities. Similarly, the applications developed for the ARM architecture cannot be executed on X86 without code modification and re-configuration.

The efficient utilization of computing resources, consisting of multi-core Central Processing Units (CPUs), Graphics Processing Units (GPUs) and Field Programmable Gate Arrays (FPGAs), has become an interesting research problem for achieving high performance on heterogeneous cloud computing platforms. In particular, FPGA and GPUs accelerators can provide significant business value in cloud environments due to its great computing capacity with predictable latency and low power consumption (Orellana et al. 2014), but paradoxically this use also directly related to the energy consumption of the system (Buyya et al., 2013), and cost. FPGA is an integrated circuit designed to be configured by the customer using a hardware description language (HDL), similar to that used for an application-specific integrated circuit (ASIC). FPGA have begun to make their way into datacentres and clouds, with several categories of use within the context of cloud-based datacentres. The first is on an infrastructure level, where FPGAs are used within the equipment that enables the datacentre itself, such as switches and routers. FPGA in this category are transparent, neither the cloud provider nor users are aware of them. The second category sees FPGAs being used as "appliances" – inside boxes that accelerate certain processes or tasks, a good example might be FPGA-based memcached appliances (Chalamalasetti et al. 2013). While appliances may be available to cloud end-users, the FPGAs inside are generally not programmable, not accessible, and essentially transparent to users. The third category sees FPGAs being made available as a general cloud computing resource, like virtual machines (VMs). In this category, a user is able to allocate FPGA hardware resources for whatever task they require, retaining the ability to program them, and using the same cloud infrastructure that manages VMs or other cloud resources. From a cloud service developers perspective, FPGA have been reserved for specialised applications where the need for custom processing hardware that can be updated on-demand outweighs the complexity in programming the hardware. While FPGAs are programmable like graphic processing units (GPU) or CPUs, they are also aimed at parallel low-latency issues for areas like inference and deep neural networks. But unlike ASIC, in FPGA, the field programmable part (i.e. algorithm) can be reprogrammed when needed. The disadvantage however with FPGA is that the programming and reprogramming is done in complex, low-level hardware definition languages like Verilog, etc. and the very different programming models used to configure these hardware is challenging for developers who are already used to higher level programming languages like C, C++ and OpenCL, which further adds another layer of complexity to the already heterogeneous cloud computing environment. The usage of FPGA for computation acceleration has made significant inroads into multiple application domains due to their ability to achieve high throughput and predictable latency, while providing programmability, low power consumption and time-to-value (Chin et al., 2014). Different types of applications can be and have been accelerated by FPGA, examples include image and video processing, real-time data analytics, ad technologies, audio, telecommunication, and even software defined networking (SDN).

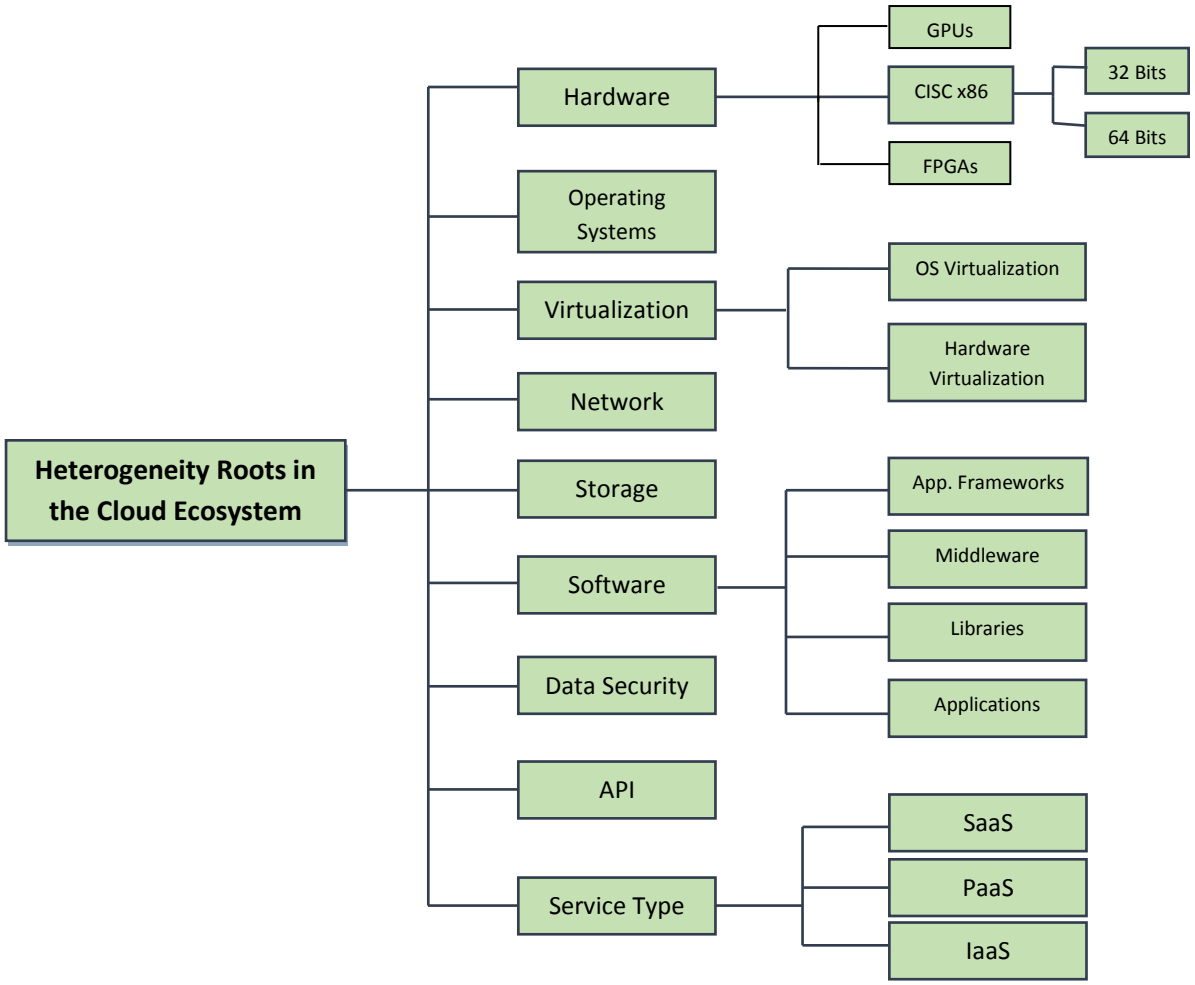


Figure 2.22-Taxonomy of Heterogeneity roots in Cloud Computing

2.7.2.2 ***Operating System Heterogeneity:*** In almost any advanced computing environment or state-of-the-art development where computers are used, heterogeneity is a fact of life (Notkin et al. 1988; Bershad et al. 1987). The major exception might be computing environments which run a single operating system or is limited to services from a single vendor. However, the fundamental problem of heterogeneity is that users require existence of a diverse set of services and applications, and the ability to construct new services and applications readily. In the cloud environment, for instance, the proliferation of different machines and operating systems is proving to be an issue to the efficient use of heterogeneous cloud services. The current challenge is that system administrators must spend considerable amount of time writing patch codes that enable specific dissimilar machines to communicate.

2.7.2.3 ***Virtualization Heterogeneity:*** Virtualization in cloud computing provides the necessary abstraction such that the underlying fabric (i.e. raw compute, storage, network resources) can be unified as a pool of resources and resource overlays (e.g. data storage services, Web hosting environments) can be built on top of them. There are notable reasons why clouds tend to adopt virtualization, a notable reason is increased application availability.

For example, virtualization allows quick recovery from unplanned outages, as virtual environments can be backed up and migrated with no interruption in service. While virtualization can also be used to abstract concerns about physical hardware heterogeneity, distinct differences exist between common hypervisors such as ZEN, KVM, VMware and others. It is also worth noting that virtualization, in the past, had significant performance losses for some applications, which has been one of the primary disadvantage of using virtualization in the first place. However, over the past few years, processor manufacturers such as AMD and Intel have been introducing hardware support for virtualization, which is helping narrow the performance gap between applications performance on virtualized resources as it compares with that on traditional operating systems without virtualization (Foster et al. 2010). In terms of heterogeneity, the difference between the choices of virtualization technology by cloud providers can hamper cross-cloud interoperability and portability, thereby intensifying the problems of virtual machine (VM) mobility. The main challenge in this regard is that live migration of VMs requires storage and network services from their hosts. Once a VM is live migrated from a host to another host, it still requires access to the storage and network services of source host. Moreover, VM migration from a source cloud to destination a destination one over a Wide Area Network (WAN) constitutes transferring memory, status, and storage of the VM. But, storage and network environments of different heterogeneous clouds are generally independent and separated by firewalls.

2.7.2.4 ***Network Heterogeneity:*** Adoption of the concepts of inter-connected data centres and server virtualization has increased network demand tremendously. Large enterprises such as Citrix, Microsoft, and VMware are deploying server virtualization technologies. In addition, other organizations are now willing to introduce new initiatives to their infrastructure that use virtualization technology concepts. Consequently, compact integration among physical infrastructure, virtual servers, and networks is required (Jammal et al. 2014). Although networking vendors have launched some innovations such as network fabric and convergence architectures to fix the scale and complexity challenges facing cloud computing services in the data centre network (DCN) infrastructure, these solutions do not address the problems in heterogeneous networks. Nevertheless, the software-defined network (SDN) paradigm is a promising solution to solve these challenges in DCN setups. The SDN approach mitigates the interconnection challenges of cloud DCNs (Pries et al. 2012). The characteristics of heterogeneous DCN architectures (e.g. VL2, Portland, and Elastic Tree) are represented by OpenFlow rules. These rules are passed to all DCN elements to implement inter-DCN connectivity (Boughzala et al. 2011). These rules support VM migration between different DCN

schemes without connectivity interruption based on re-routing mechanisms. Network connectivity over distributed cloud resources in different providers, is a challenging issue for both cloud consumers and providers. To tackle this challenge, the concept of seamless connectivity among heterogeneous network technologies plays a vital role that necessitates reliable intra-system and intersystem handoff schemes (Mann et al. 2012). Intra-system handover is a less challenging task due to inward homogeneity of engaging technologies, while addressing inter-system handover is more complicated due to signal transmission difficulties between heterogeneous environments. To realize seamless connectivity across heterogeneous wireless networks, the burgeoning concept of next generation wireless networks (Oltsik and Laliberte, 2012) with the notion of all IP-based infrastructures is emerging. In the absence of seamless connectivity, the quality of user experience is decreased because of decrements in communication quality and increments in code execution and application response time.

2.7.2.5 ***Storage Heterogeneity:*** Storage solutions hosted within internal network-attached storage (NAS) or storage area networks (SAN) facilities must continue to support the same storage and access needs regardless of which cloud storage provider is selected. Storage requirements will vary for different types of data. Structured data will most often require a database system, or require application specific formats. Unstructured data will typically follow any number of common application formats used Word Processors etc. Many Cloud Services are available today, such as Amazon EC2, Google App Engine, Dropbox, or SoundCloud, supporting a multitude of different services, but also presenting heterogeneous characteristics on how they are accessed via different APIs, or which functionality they offer. However, despite the observed heterogeneity, one common aspect is that nowadays cloud services provide a large amount of storage, directly or indirectly. The former is termed generic cloud storage services, because they accept to store data represented in any data type (e.g., Dropbox, Amazon S3). Whereas the latter is termed data-specific cloud storage services because they accept to store data only represented in specific data types (e.g., Google Picasa, SoundCloud). The heterogeneity among generic and data-specific cloud storage services turns the task of aggregating (i.e. dynamically configure and bundle) cloud services' storage into one single storage entity a challenging task. Furthermore, there are large differences in I/O speeds from local disk storage to wide area networks, which can drastically affect application performance. To achieve good scalability at Internet scales for clouds and their applications, data must be distributed over many computers, and computations must be steered towards the best place to execute to minimize the communication costs. The main heterogeneity challenge for efficient scaling of applications is the location of the data relative to the available

computational resources – moving the data repeatedly to distant CPUs is becoming the bottleneck (Foster et al. 2010).

2.7.2.6 ***Software Heterogeneity:*** Systems in the cloud may reside on disparate platform architectures. Different platform providers offer different cloud applications frameworks and differences do exist between them that affect interoperability. Most applications exhibit properties of multiple modalities of scale (horizontal and vertical) which are however difficult to identify. The architectural choices of the infrastructure thereby influence immensely what kind of qualities can be expected for the different applications. Moving to the cloud or changing to a new service provider within the cloud can be impacted by architecture differences. Leading platforms such as Google App Engine (GAE), Force.com and Amazon all provide some degree of support for moving applications. However, each is architected differently making moving from one to another a difficult and error-prone task. As an example, GAE uses a modified Python runtime and chooses Python scripting language for Web application development. The interface to its underlying BigTable storage system is a proprietary query language (named, GQL) that is reminiscent of SQL. Cloud providers (such as Amazon Web Services, Microsoft's Azure Services Platform) have generally adopted Web Services APIs where users access, configure and program cloud services using pre-defined APIs exposed as Web services. HTTP and SOAP are the common protocols chosen for such services. Although clouds adopted some common communication protocols such as HTTP and SOAP, the integration and interoperability of all the services and applications remain the biggest challenge, as users need to tap into a federation of clouds instead of a single cloud provider. To be more concrete, in the context of software heterogeneity, understanding and clarifying the specific portability and interoperability concerns is the first step to avoiding the risk of vendor lock-in. For this reason, we highlight several important items to consider such as: 1) use open and published API's to ensure broad interoperability between software components and to facilitate migrating applications and data should changing a service provider become necessary; 2) investigate the cloud provider's APIs to determine where differences lie and plan for any changes necessary; 3) applications in the cloud interoperate over the Internet and outages can occur. So, it is important to determine how failure in one component will impact others. Moreover, communication between clouds typically has a high latency which makes synchronization difficult; and 4) due to the absence of data interoperability interfaces, data components interoperate via application components rather than directly. Hence, making data synchronization an issue of importance when components in different clouds or identical resources work together, whether they are identical.

2.7.2.7 ***Data Security Heterogeneity:*** Cloud computing mostly comprises dedicated data centres belonging to the same organization, and within each data centre, hardware and software configurations and supporting platforms is in general more homogeneous as compared with those in grid environments (Foster et al. 2010). Data and applications in the cloud reside on systems consumers do not own and likely have limited control. Interoperability can become a serious issue for cross-data centre, cross-administration domain interactions; for instance, imagine running an accounting service in Amazon EC2 while other business operations are run on Google infrastructure. Being that security is one of the main concerns for the adoption of cloud computing, a number of important items to consider for interoperable security include: 1) ensure authentication controls for system and user account access credentials are compatible to protect continued and consistent system access integrity and security; 2) protect sensitive data moved to the cloud through interoperable encryption that directly and persistently protect data and files regardless of the platform, storage systems, or location where it resides; 3) for applications utilizing SOA, compensate by ensuring data is protected through portable encryption formats; 4) API security keys used for calls to services requiring authentication should interoperate and appropriate maintenance and protections of keys must exist on new platforms; 5) data integrity measures should be incorporated to ensure data remains unaltered while in the cloud; and 6) since cloud consumers will not know where their data will be stored, it is important that the cloud provider commit to storing and processing data in specific jurisdictions and to obey local privacy requirements on behalf of the customer (Chetan et al., 2010).

2.7.2.8 ***API Heterogeneity:*** Most cloud providers develop and deploy their own proprietary APIs to describe syntax of specific operations to be utilized by their clients. A drastic growth in the number of cloud providers has created a huge silo of different APIs that intensifies the difficulty of developing applications due to interpreting semantics of data and operations. It is obviously complicated by issues such as multiple administrative domains; large variations in resource heterogeneity, stability and performance; exception handling in highly dynamic (in that resources can join and leave on-demand) environments, etc. (Foster et al., 2010). This outlook, results in API variation intensifying interoperability and portability issues. To mitigate the impact of API heterogeneity on the cloud, several regulatory and research unions endeavour to provide common cloud APIs through, including the European Telecommunications Standards Institute Technical Community (ETSI TC Cloud), DMTF, and Cloud Audit.

2.7.2.9 ***Service Type Heterogeneity:*** Service heterogeneity in the cloud domain arises from variations in the services (e.g. infrastructure, platform, software and security) offered by different vendors. For example, Google App Engine (PaaS vendor) and Microsoft Windows Azure (PaaS) provide dissimilar security features; though they offer paid backup storage service, critical data privacy is only offered by Azure (Sanaei et al. 2014). Therefore, users, especially corporate users, face difficulties in moving from one vendor to another. Although cloud computing provides services at three different levels (IaaS, PaaS, and Saas), standards for interfaces to these different levels remain to be defined. This leads to interoperability problems between today's cloud services, and there are little business incentives for cloud providers to invest additional resources in defining and implementing new interfaces. While many types of cloud computing components can have simple interfaces that can be defined in standards to which all instances can conform. This is, however, not the case for applications, as each application is different. There is reason to standardize the interfaces to some applications to enable collaboration across industry sectors, but otherwise it is desirable to allow variations, so that the interfaces can reflect specific product functionality, and individual vendors are free to introduce the functionality that they believe meets the needs of their customers (Open Group, 2013). As cloud computing market, mature, and more sophisticated applications and services emerge that require multi-cloud collaboration, there will be growing incentives to adopt standard interfaces that facilitate interoperability to capture emerging and growing markets in a saturated cloud ecosystem.

2.7.3 Approaches for Tackling Heterogeneity Roots in Cloud Computing Environments

A major appeal of cloud computing is that it abstracts hardware architecture from both end users and programmers. This abstraction allows underlying infrastructure to be scaled up or improved without forcing changes in applications (Crago and Walters, 2015). However, developing cloud computing applications and technology compatible with datacentre heterogeneity will require finding ways to optimally exploit varied special purpose processing elements without losing the advantages of abstraction. For example, the SaaS model provides developers the most flexibility because heterogeneity can be hidden within the application software and not exposed to end users. Still, software developers building SaaS applications and/or platforms must keep in mind heterogeneous architectures like those that IaaS and PaaS deliver, and so must address issues involving implementation portability and scalability. Common challenges in this aspect will likely be specific to the software (SaaS) service under development, but will involve making engineering choices about whether to use existing IaaS or PaaS interfaces or to devise custom implementations that target heterogeneity. To this end, we present the different approaches for tackling such heterogeneity problems specific to cloud computing environments.

- *Adoption of Standards*: different forums, organizations and regulatory organisations are trying to define a set of standards and guidelines for defining the most relevant aspects of cloud computing, such as virtual machines management, classification of services and features, protocols, or federation capabilities (Miranda et al., 2013). These attempts have great difficulties in being widely accepted, mainly caused by each vendor's interest in keeping their customers tied to their products. Nonetheless, if cloud providers where to use common standards, both seamless integration amongst providers and portability become straightforward. However, standardization is not an appealing solution for some cloud providers (Petcu, 2011).
- *Usage of Intermediary Layers*: For example, reducing accidental complexity, by adopting semantics and model-based solutions (Gonidis et al., 2012). This approach is based on software adaptation and Model-driven engineering (MDE). It describes a lightweight alternative for designing and building loosely coupled cloud applications composed of components that are grouped and distributed amongst different cloud environments. Due to the heterogeneity of the services and interfaces provided by such environments, components must be properly adapted to each environment considering the technical differences or mismatches that exist in each case. The adaptation process guarantees that each component continues to provide its part of the application's behaviour and that it interoperates correctly with its dependant components. According to (Miranda et al., 2013), the most outstanding benefit of using adapters in cloud environments is the ability to automatically generate loosely coupled applications with a reduced impact on their deployment, and at the same time favouring cloud interoperability. However, this solution has not yet been thoroughly explored.
- *Adoption of High Abstraction Layers or Middleware's*: the lack of standards has motivated the emergence of alternate solutions. Most of them rely on the use of an intermediate layer that lies between the consumer and the provider to abstract the former from specific implementations. An abstraction layer hides the differences between providers and exposes a uniform semantics and syntax. Limitations of abstraction layers include maintenance in response to changes made by a cloud provider, and the limited coverage of provider functionalities. Several middleware-oriented approaches have been explored and developed amongst the literature (Maximilien et al., 2009) and research projects (Mohagheghi and Sther, 2011 & Martino et al, 2011), providing encouraging results. However, middleware solutions are often quite complex and heavyweight. Considering that they should be deployed in conjunction with the application, they will clearly penalize the performance of the software components attached to them. Further yet, the source code of the middleware-dependent components will be tightly coupled to the specification of the middleware, thereby moving the lock-in effect from vendors to middleware (Miranda et al., 2013).

2.8 Cloud Computing Migration

Enterprises are attracted by cloud offerings, since they can take immediate advantage of instant scalability and elasticity, isolated processes, reduced operational effort, on-demand provisioning and automation. However, while these advantages are compelling, important factors like the actual migration task are often neglected. Yet, overcoming such migration impediments can become a laborious and costly endeavour, especially for smaller companies with inherently less financial power (Zenga et al., 2010). Many businesses are in search for better ways to migrate their existing IT assets to a cloud-based infrastructure with minimal effort, so that they can reap the benefits the cloud proffers. The reasons for such move to the cloud will vary from business to business. Thus, each business will make cloud decisions based on differing needs and objectives. However, decision making when selecting suitable cloud service and deployment models requires analysis of which cloud model is the best fit for a defined need. For instance, an organisation looking to host business processing in the cloud may choose the IaaS model to extend their infrastructure needs for OS platform support, storage, email and messaging etc. On the other hand, companies needing application support may decide on the SaaS model to access business application services for functions such as Customer Relationship Management (CRM), business collaboration software, or Ecommerce. Those looking to expand or move custom application processing to the cloud may look to the PaaS model for cloud development frameworks.

The ability to move to the cloud requires that applications now hosted internally can run in the cloud. This implies application that worked on in-house infrastructures must continue to work with the same capabilities and reliability as they move to the cloud. In other words, applications built on cloud frameworks must meet the same business requirements and development efficiencies as in-house efforts. Likewise, storage solutions hosted within internal (NAS or SAN) facilities must continue to support the same storage and access needs despite which cloud storage solution or provider is selected. Once established, each of these scenarios must also provide on-going compatibility should changing business needs require changing any of the underlying cloud components (i.e. hardware, OS, virtualization, networks, storage, software etc.) on which a solution depends. A factor for successful cloud deployment is achieving processing compatibility for cloud systems with that of the traditional systems they replace. In agreement with Banerjee (2012), while much research has been discussed about the benefits of cloud computing and the implementation details, there still exists some gap when it comes to giving direction to enterprises on how to migrate an organisation's IT resources to cloud environment. Moreover, it is true that some IT assets currently deployed in company data centres or co-located facilities might not make technical or business sense to move to the cloud or at least not yet (Varia, 2010). However, there are several assets within an enterprise that can be moved to the cloud with minimal effort. For example, applications (with

unpredictable or cyclical usage patterns) designed to spread their workload across multiple servers will be able to benefit from automated scaling of resources to match the current demand. This behaviour, combined with pay-per-use characteristic of a cloud, can lead to significant financial savings for the enterprise. Despite this fact, the skills and technology to assess the options, costs and benefits of different clouds intelligently, then select and execute the move may be scant or non-existent. In this regard, the focus of discussion presented below is more on how to move or replace organisations existing IT assets with cloud computing SaaS alternatives with minimum effort.

2.8.1 Migrating to SaaS Cloud Environments: An Overview

Over the last decade, SaaS delivery has outpaced traditional software application delivery, growing nearly five times faster than the software market and has become a significant growth driver for the expansion of all software market (McGrath and Mahowald, 2015). The adoption rate and market interest for migration to cloud computing SaaS offerings is attributed to the rapid growth of the Internet, advances in telecommunication technologies and decrease in bandwidth costs, as well as the increasing use of productivity tools for the web (Dubey and Wagle, 2007).

The business model for cloud-based SaaS services has several characteristics that differentiate it from traditional on-premise software. From the cloud service consumer perspective, software applications from cloud SaaS vendors are offered as 'experience goods' to the enterprise that use them. The term experience goods in this context imply that it will take a while for the cloud service consumer to figure out how well the software product will work within their existing on-premise ICT components. In other words, the cloud service consumer must then figure out the functionality requirements of SaaS applications and match them to their respective business needs, and subsequently understand how they can be integrated into existing legacy systems (on-premise) and technical infrastructure. However, to take advantage of cloud computing environments and protect existing investments to legacy systems, enterprises are eager to replace and/or migrate legacy systems to the cloud. So far, the amount of research effort in this aspect of cloud computing (e.g. Khajeh-Hosseini et al. 2011; Ward eta al. 2010; Menzel and Ranjan, 2012; Binz et al. 2011; Barbar and Chauhan, 2011) focus more on decision making support for cloud migration in enterprise as benefits, risks, costs, and organisational and socio-technical factors must be considered before migration. Hitherto, some innovative methods have been proposed, related tools have been developed, and lots of organisations have made some trials in migrating to SaaS cloud computing services. Per Zhao and Zhou (2014), migration to SaaS cloud computing environments can be divided into three sub-strategies concretely, namely 1) replacing by SaaS, 2) revising based on SaaS, and 3) reengineering to SaaS. In fact, enterprises often migrate their on-premise systems to cloud environments by adopting the first sub-strategy.

To the first sub-strategy, legacy system will be completely replaced by commercial software delivered as a cloud service. Based on the second sub-strategy, some functionality of on-premise systems will be replaced by cloud service, though the legacy system need to be adapted per the target SaaS platform. To the third sub-strategy, legacy systems will be reengineered to cloud service, but if the legacy system is replaced by commercial software delivered as a service, the migration effort will be reduced greatly and reengineering process may be unnecessary. Cloud migration (Jamshidi et al. 2013) benefits from the cloud promise of converting capital expenditure to operational cost (Armbrust et al. 2009). In **Table 2.3**, we compare the characteristics of these three SaaS migration sub-strategies and map them to the four identified migration types proposed by Andrikopoulos et al. (2013).

Table 2.3 Comparison between the Cloud SaaS Migration Strategies

Migration Characterisation			
SaaS Migration Strategies	Revise for SaaS	Replace with SaaS	Re-engineer to SaaS
Migration Type(s)	Type I	Type II, Type III	Type IV
Migration Workload	Little	Moderate	Much
Migration Complexity	Easy	Moderate	Difficult
Adaptation Needs	No need	Service and data integration, service composition	Reverse engineering, redesign structure, forward engineering
Effect	Flexible pricing mechanism and convenient maintenance	Same as revise but with additional reuse	Same as replace but with scalability in addition
Disadvantages	Migration is unable to take full advantage of the cloud platform	Missing capabilities, transitive risks and framework lock-in	Major barriers in the engineering process e.g. multi-tenancy, configurability etc.

2.9 SaaS Migration Strategies

A clear perspective of the main migration types regarding SaaS and on how they can be organised to ease decision making is the primary step for having a comprehensive overview of the status of cloud computing SaaS migration. To distinguish between different types of cloud migration, in this sub-section we borrowed the classification proposed by Andrikopolos et al. (2013), as shown in **Figure 2.23**, which considers different application layers and different degrees of adaptation required to enable migration. These different migration approaches are explained later in **Section 2.9.2**. Looking into how applications are usually built, i.e. using the three layers pattern (presentation, business logic, and data), as shown in **Figure 2.23**, it can be seen that it is possible to migrate only one or more architectural layer(s) to the cloud instead of the whole application (Fowler, 2012). While the economic reasons and business case(s) for cloud migration is compelling, the lock-in challenges it poses are equally evident. Hereof, we argue that SaaS cloud services pose several data, application (and contract) lock-in risks for cloud customers and developers due to issues related to governance, losing control over redundancy, location, relevant configurations as well as losing administrative and

security controls in cloud computing solutions. Some of these lock-in risks are not fundamentally new but are fundamentally intractable in the cloud environment. In some cases, the customer(s) cannot easily extract their data and application programs from one SaaS provider environment to run on another. Moreover, concern about the challenges of extracting data from the SaaS cloud is preventing some organisations from adopting cloud computing (Armbrust et al. 2009).

So, given that each organisation is unique with its own requirements and challenges per cloud services, it is therefore useful to evaluate SaaS products for potential lock-in risks and come up with a strategy that tackles their unique requirements and implementations. For instance, if the business needs to migrate to a SaaS solution is unique to a single organisation or if other companies with similar business needs are neither prepared nor incentivized to replace a vertical SaaS application then the solution should be considered a sector-specific one. In which case, the solution decision may be quick and the path from procurement to implementation should be as easy and smooth as possible. Whereas, if multiple companies identify a common business need that could be addressed by a candidate (horizontal SaaS) application, business stakeholders from across the enterprise will need to come together to determine if an appropriate SaaS solution is available. In this case, the decision process is longer but once a solution is determined, the procurement to implementation process should be as streamlined as possible. In this aspect, the IT maturity of an organisation along with its size will significantly impact the SaaS service model decisions.

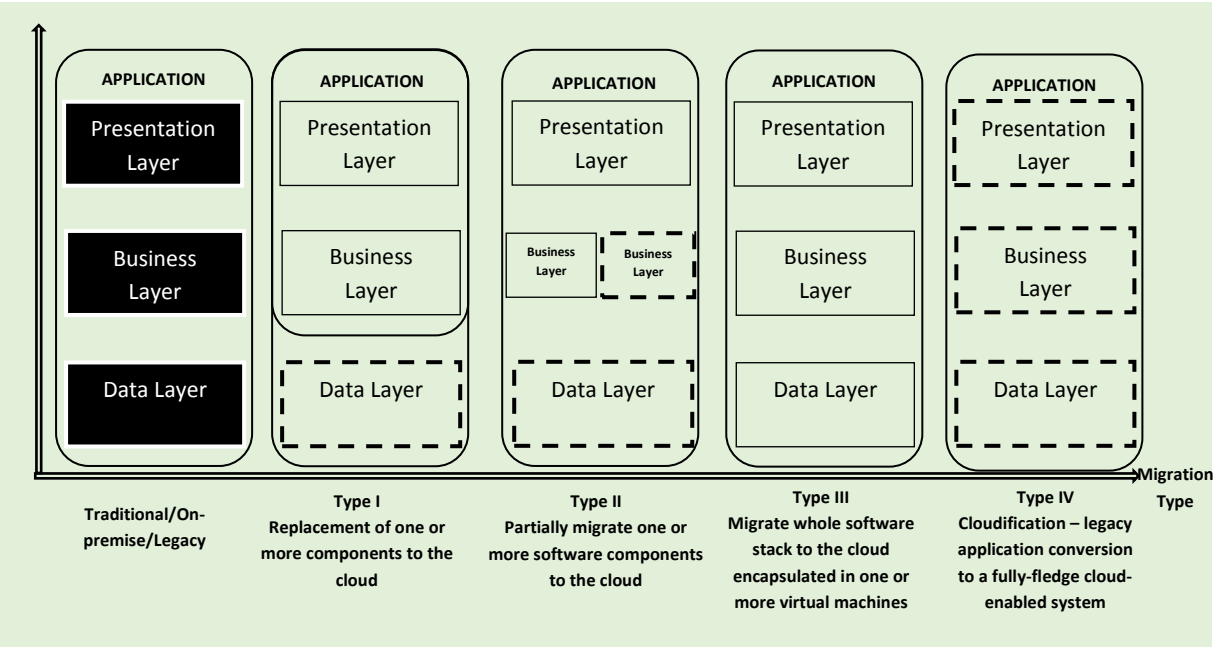


Figure 2.23-Different Types of Cloud Migration (Andrikopolus et al. 2013)

The approach for adopting SaaS offerings will differ based on the IT maturity of the organisation. To help companies assess where SaaS is a strong fit, identify readiness to adopt SaaS for

a specific purchase, and address hurdles to SaaS success, we incorporated the SaaS capability maturity assessment proposed in (Herbert, 2013) into our study. In corroboration with Herbert (2013), it is recommended that before purchasing/adopting a cloud SaaS solution, organisations should determine whether: 1) the solution category is a good candidate for software-as-a-service replacement; 2) the SaaS solution has the requisite technical capabilities to support the business requirement; 3) the organisation has development skills suitable for SaaS; 4) the organisation has an appropriate solution governance process to capitalise on the benefits of SaaS; and 5) the SaaS purchasing processes are sound. In addition, customers can negotiate contract terms to reduce SaaS lock-in risks by including the right to export data from the system in standardised formats and long-term pricing and support agreements. The next section presents the two main migration strategies that represent the spectrum of cloud migration alternatives.

2.9.1 Architectural Solutions for Migrating into SaaS Cloud Environments

Cloud migration within an enterprise context could be referred to as either architecture or operations migration. The former involves migrating legacy applications to a scalable, cloud-ready architecture, often using newer languages (e.g. Google's Go and Apple's Swift) and newer components such as NoSQL databases (Weinman, 2016). Whereas the latter involves migrating either such cloud-ready applications (e.g. SaaS applications) or newly designed and coded applications from a private cloud to the public cloud or vice versa, or among public clouds. Moreover, this latter migration approach might itself require different APIs and recoding, or it might be made easier using standard stacks or services (e.g. Open Stack or Hadoop). The economy of scale of the first type of migration do not always favour application rewrites since the upfront cost to re-architect and rewrite an existing application may not generate a sufficient stream of benefits for the service consumer. However, cloud-ready applications are built out of composable objects or services that can independently scale (e.g. Web tier and database layer with a load-balancing layer capable of scaling independently on the number of users and on the quantity of data or reads and writes). Emerging approaches in this direction may include micro-services and new approaches such as Amazon Web Services Lambda functions.

Today, most enterprises have a mix of standard and customised applications. Customised applications will usually remain in the enterprise pending the degree of customisation, while standard applications might need to remain in the enterprise, depending on the data location, its specific requirement (including interoperability, portability, integration, security and privacy aspects), and how much of it there is (Yousif, 2016). Enterprises should always conduct extensive due diligence before attempting to replace or migrate applications to the cloud because cloud migration is not without pitfalls. Besides, cloud migration usually involves considerable manual processes, which are prone to error. Further, enterprises should also consider experimenting or start small and increase the migration as they build required in-house expertise. Conclusively, for organisations planning to adopt

and migrate to cloud-based services, many factors, both technical (e.g. migration effort, environmental constraints, switching costs, performance impact) and non-technical (e.g. security risks, operational costs, business gain, and contract lock-in) need to be evaluated prior to service migration. Identifying these multi-dimensional factors, examining potential migration constraints and adopting a suitable architectural solution are requisite steps to facilitate successful application migration to/in the cloud (Jadeja and Modi, 2012). In this section, we distinguish between two migration strategies; cloud hosting and cloudification. These two strategies represent the spectrum of cloud migration alternatives (Khajeh-Hosseini et al. 2011) being studied in both academia (Jamshidi et al. 2013; Bitzer, 2004) and industry (Kolb and Wirtz, 2014; Sun and Li, 2013).

i. **Cloud Hosting:** This refers to the decision of cloud service consumers (e.g. developers) with regards to right architectural solutions to properly host a given application component or data in the cloud. Such decisions will depend on the constraints the cloud service provider imposes on the cloud's operational environment and how those constraints affect the target software components deployment and execution. Some of the commonly available architectural solutions for cloud hosting are as follows: rebinding, service adaptation, service conversion and compensation.
ii. **Cloudification:** Typically, it involves replacing one or more application components with existing cloud services that offer similar or related functionality. This functionality has two main requirements. First, there should be a candidate cloud service(s) to replace each of the targets components. Secondly, the target components' current state must be transferable to compose the state of the corresponding services in the cloud. Cloudification strategy usually involves one of the following architectural solutions: replacement, interface adaptation and interface conversion.

Across the two broad migration categories, identifying the most suitable architectural solutions for a given cloud migration scenario should also consider other potential system-wide (or cross-cutting) issues (such as interoperability, portability, integration, security, standards etc.) related to the overall migration process. However, no single migration strategy is likely to meet all an organisation's technical and business needs. For this reason, it is expected that companies may use a combination of architectural (i.e. hybrid) solutions and deployment models as part of their cloud migration decisions. Therefore, understanding these migration strategies and their respective architectural solutions will assist cloud service customers and enterprises in determining how to correctly and securely migrate existing applications and data to the cloud. Further, competing architectural standards are already being developed, including Open Virtualization Format, Open Cloud Computing Interface (OCCI) (2016), Data Liberation Front (Google, 2016), SNIA Cloud Data Management Interface (CDMI) (2012) and OASIS Security Assertion Markup Language (SAML)

(2015) with major cloud vendors selling their own mutually incompatible de facto standards. Limitations include differences between common hypervisors (at the IaaS level), gaps in standard APIs (at PaaS and SaaS level) for management functions, lack of commonly agreed data formats and issues with machine-to-machine interoperability of web services (at SaaS and IaaS layers). The next section presents brief analyses of some core lock-in challenges with switching cloud SaaS vendors.

2.9.2 Cloud Computing Migration Types

Migrating IT assets into cloud models is inherently an application centric activity where each image/instance in the cloud typically runs a single application workload (Banerjee, 2012). Application migration is the process of redeploying an application, typically on newer platforms or infrastructure. As such, migrating enterprise IT applications to cloud environments need to follow a multi-step process to get those applications running correctly in the targeted cloud environment. Many organisations are taking incremental approach to cloud migration. To identify applications for migration to a cloud, it is necessary to first understand the business and technical factors for the migration. First, the targeted application must be identified and segregated from other applications running on that same server. The target infrastructure can be a public, private, or hybrid cloud. Additionally, the application can involve a physical-to-virtual (P2V) migration, for instance, if the application is not running on a virtualised platform (Cisco, 2010). Then an image of that application, its Operating System (OS) and infrastructure management agent need to be created and added to the cloud catalogue. Finally, the image needs to be represented in the cloud environment and verified to run with acceptable Quality of Service (QoS) characteristics.

Decisions to migrate enterprise business systems in the cloud environment (i.e. cloud migration) can be complicated as evaluating the benefits, risks and costs of using cloud computing is far from straightforward. Organisational and socio-technical factors must also be considered during the decision-making process as the transition to the cloud is likely to result in noticeable changes to how systems are developed and supported. Cloud migration facilitates the adoption of flexible cloud computing services, thus it requires an explicit analysis, exact planning and execution prior to migration to ensure the solution on demand. Choosing which application component to migrate to the cloud or replace with an appropriate cloud service is crucial, and the decision can affect the entire migration process. To distinguish between the different approaches for migrating an existing application to (or in) the cloud, five migration options are defined below:

- **Type I – Re-host** (on IaaS): implies redeployment of the application to a different hardware environment and changing the application's infrastructure configuration. Re-hosting an application without making changes to its architecture can provide a fast cloud migration solution. Virtual machine (VM) image format and management API lock-in risk.

- **Type II – Refactor** (for PaaS): describes running an application (usually Web applications on the cloud provider's infrastructure. The primary advantage is blending familiarity with innovation as "backward-compatible" PaaS means developers can reuse languages, frameworks, and containers they have invested in, thus leveraging code the organization considers strategic. Disadvantages include immature PaaS offerings with missing capabilities and framework lock-in.

- **Type III – Revise** (for IaaS or PaaS): means to modify or extend the existing codebase to support legacy modernization requirements, the use re-host or refactor options to deploy to the cloud environment. This option allows organizations to optimize the application to leverage the cloud characteristics of providers' infrastructure. Depending on the scale of the revision, revise is the option likely to take most time to deliver its capabilities.

- **Type IV – Rebuild** (on PaaS): requires architecting the application for a new container (e.g. from Java to .Net) environment. Although rebuilding requires losing the familiarity of existing code and frameworks, the advantage of rebuilding an application is access to innovative features in the provider's platform. They improve developer productivity, such as tools that allow application templates and data models to be customized, metadata-driven engines, and communities that supply pre-built components. However, lock-in is the primary disadvantage so if the provider makes a pricing or technical change that the consumer cannot accept, breaches service level agreements (SLAs), or fails, the consumer is forced to switch, potentially abandoning some or all its application assets.

- **Type V – Replace** (with SaaS): involves discarding an existing application (or set of applications) and use commercial software delivered as a service to satisfy those business requirements. For instance, using a web mail service (Gmail by Google or LiveMail by Microsoft) instead of a local email server. This option avoids investment in mobilizing a development team when requirements for a business function change quickly. It is the simplest form of Cloudification – replacing one or more application components with existing cloud services that offer similar related functionality. Typically, existing data requires migration to the SaaS environment. Application data import/export is achieved with an API or configuration/admin console. However, the replacement option is only feasible if the target component and the candidate cloud service have identical or fully compatible interfaces. Disadvantages can include possible data lock-in (except the migration plan includes a flexible schedule for discontinuing replaced applications), difficulty to integrate with existing systems and processes, inconsistent data semantics, data access issues, incompatible process, policy or data models, difficulty to customise or reconfigure, and vendor lock-in.

2.9.3 Cloud Migration Patterns

There is no doubt that deploying applications in the cloud can lower infrastructure costs and increase business agility within the enterprise. Based on the background research in the preceding section, there are some common themes that have emerged for migration to cloud computing. These themes are rooted in the work by (Banerjee, 2012a), and are described here in the context of five steps of moving workload to the cloud, as depicted in **Figure 2.24**. However, when compared to a phased-driven approach to cloud migration proposed by (Varia, 2010), the five steps in **Figure 2.24** slightly changes to six phases, as illustrated in **Figure 2.25**.

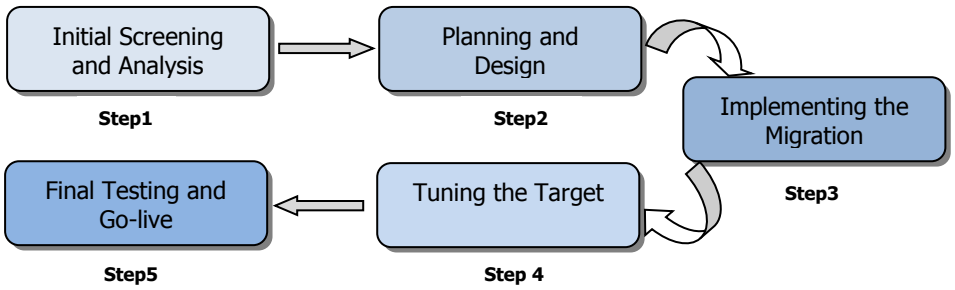
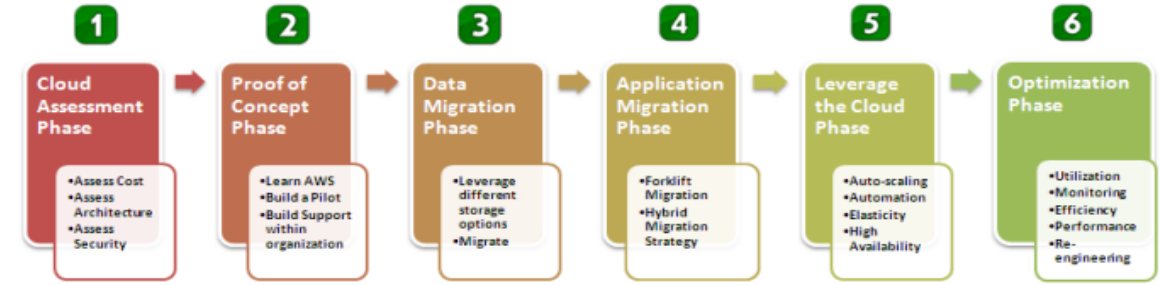


Figure 2.24- The Five Step Methodology to Cloud Migration (Adapted and Modified from [Benerjee, 2012])



Phases	Benefits
Cloud Assessment • Financial Assessment (TCO calculation) • Security and Compliance Assessment • Technical Assessment (Classify application types) • Identify the tools that can be reused and the tools that need to be built • Migrate licensed products • Create a plan and measure success	Business case for migration (Lower TCO, faster time to market, higher flexibility & agility, scalability + elasticity) Identify gaps between your current traditional legacy architecture and next -generation cloud architecture
Proof of Concept • Get your feet wet with AWS • Build a pilot and validate the technology • Test existing software in the cloud	Build confidence with various AWS services Mitigate risk by validating critical pieces of your proposed architecture
Moving your Data • Understand different storage options in the AWS cloud • Migrate fileservers to Amazon S3 • Migrate commercial RDBMS to EC2 + EBS • Migrate MySQL to Amazon RDS	Redundancy, Durable Storage, Elastic Scalable Storage Automated Management Backup
Moving your Apps • Forklift migration strategy • Hybrid migration strategy • Build "cloud-aware" layers of code as needed • Create AMIs for each component	Future-proof scaled-out service-oriented elastic architecture
Leveraging the Cloud • Leverage other AWS services • Automate elasticity and SDLC • Harden security • Create dashboard to manage AWS resources • Leverage multiple availability zones	Reduction in CapEx in IT Flexibility and agility Automation and improved productivity Higher Availability (HA)
Optimization • Optimize usage based on demand • Improve efficiency • Implement advanced monitoring and telemetry • Re-engineer your application • Decompose your relational databases	Increased utilization and transformational impact in OpEx Better visibility through advanced monitoring and telemetry

Figure 2.25- A Six-step Phase Driven Approach to Cloud Migration (Adapted from [Varia, 2010]).

2.9.4 Life cycle for Managing Enterprise Cloud Migration Projects

A successful cloud migration largely depends on three things; 1) the complexity of the application architecture, 2) how loosely coupled the application is, and 3) how much effort is required to be put into migration (Cisco, 2010). However, there are also many challenges to successfully deliver cloud-based services including lock-in, security, interoperability and portability issues, data ownership, contractual issues etc. These challenges need to be understood and managed before attempting to take advantage of the benefits the cloud offers (Conway and Curry, 2012). Thus, an emerging need arises to define a management framework for how cloud migration projects can be systematically managed. In this respect, a nine-step (with four core phases) cloud life cycle approach that can be used for both the migration and on-going management of cloud-based services within the enterprise is presented in **Figure 2.26**. For detailed explanation of each of the steps, please refer to the work by (Conway and Curry, 2012).

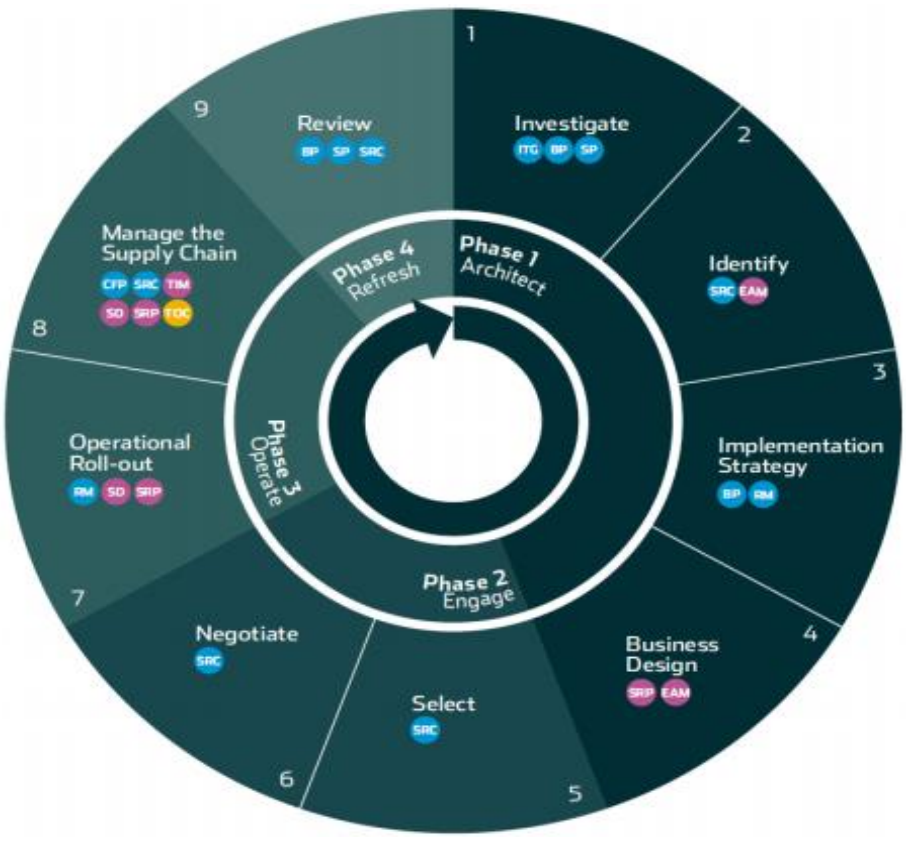


Figure 2.26-Life Cycles for Managing Enterprise Cloud Migration (Adapted from [Conway and Curry, 2012]).

The cloud life cycle is made up of nine steps (as illustrated above), broken down into four phases as concisely explained below:

1. **Phase 1 (Architect):** The first phase starts with the investigation and planning of the cloud project. It provides an insight into and an understanding of what an organisation wants to achieve by moving to the cloud, and what goals and expectations to be met.

2. **Phase 2 (Engage):** The second phase selects a service provider that can deliver the required cloud service. Selection of the best service provider is based on value, sustainability, and quality. A major challenge found in this phase is that the cloud providers contract, SLA and pricing are often delivered as standard offering to its service consumers. In effect, many organisations decide to stop at this stage, either because appropriate cloud services are not available, or because there is no cloud provider that they have confidence in to deliver the required cloud service.

3. **Phase 3 (Operate):** The third phase is the implementation and day-to-day management of the cloud service. This will require the transition of the service itself, the management of staff impacted, communication to all stakeholders, knowledge retention/transition, and acceptance sign-off. Research shows that many enterprises that had experienced smooth transition in this phase are due to, good planning, the full engagement of users, and a strong partnership with the supplier. It is equally important to manage the new cloud service as efficiently and effectively as possible. This will require effective monitoring and control so that issue, variations and disputes can be resolved to the satisfaction of both parties.

4. **Phase 4 (Refresh):** The fourth phase is the on-going review of cloud services. The cloud service requirements are reviewed based on the service itself, other changes within the enterprise, changes within the cloud provider/vendor organisation, or the need to change the supplier. Core challenges likely to be faced by enterprises in this phase are related to difficulties to integrate services due to vendor lock-in and well as not investing sufficient resources with the correct skills to decide what was needed for the future. In one instance, it was found that cloud services were being purchased in the enterprise without any central control, leading to an unfavourable mixture of solutions that was very difficult and complicated to integrate (Conway and Curry, 2012; Curry et al. 2010).

2.9.5 Decision Support for Enterprise Cloud Migration

There are many different aspects to consider when making decisions in support of selecting, evaluating, and planning the migration of an enterprise IT asset to a cloud. Generally, the process begins with analysis of the factors for the migration (application/data) and comparison of these factors to different types of cloud computing operating environment. The next step is to analyse and application details that help in building a sufficient migration plan, as well as a plan for testing each phase of the migration. This process often, as shown in **Figure 2.27**, is iterative, since data might be

uncovered that leads to the re-evaluation of the results in prior phases. While this is not a one size fits all approach, but the best practices recommended herein will help organisations identify application suitability and perform a smooth migration (Cisco, 2010).

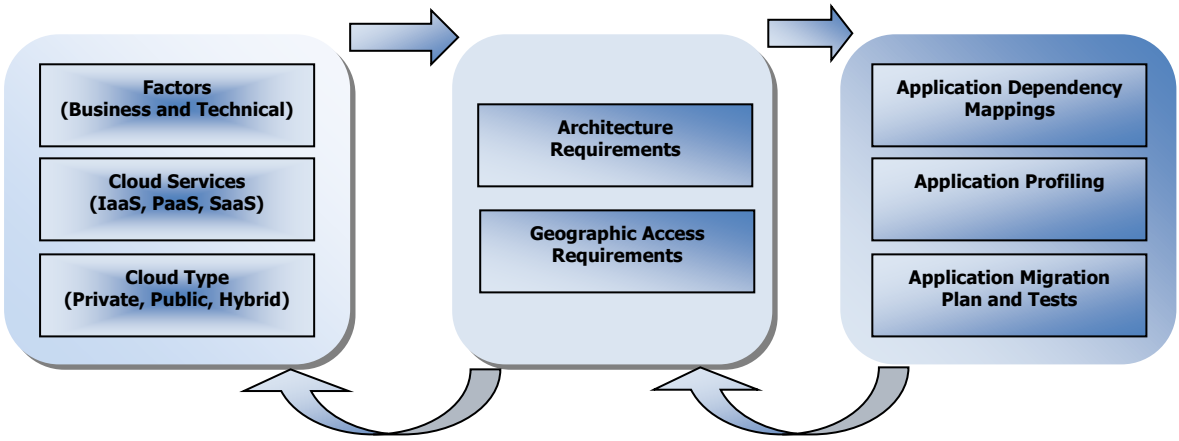


Figure 2.27- Supporting the Cloud Migration Process (Adapted from [Cisco, 2010]).

2.9.6 Drivers for Cloud Migration

Taking advantage of the capabilities offered by cloud computing requires either an application to be built specifically for it, or for existing applications to be migrated (fully or partially) to it. Cloud computing is seeing an increasing attention that is inevitably driving businesses to migrate existing on-premise applications onto the cloud (Peddigari, 2011). The foremost drivers for cloud computing are consequential cost advantages (Nussbaumer and Liu, 2013). Due to the limited financial resources of SMEs, compared to their larger counterparts, the cost factor seems to be even more crucial for these smaller companies (Chien & Chien, 2010; Sultan, 2011). Given their limited financial power, such companies cannot undertake large investments and therefore face significant advantages in adopting the cloud, as there is little or no upfront investment necessary (Daneshgar et al., 2011). The enterprise therefore gets to turn their capital expense into a variable operating expense (Khanapurkar, 2011). This fact is especially important for SMEs that have neither the required capital nor the willingness to afford expensive IT infrastructure. Additionally, whereas large corporations need to operate and manage expensive legacy systems, SMEs are less likely to have such major infrastructure, hence the overall costs can be potentially lower (Grabova et al., 2010). On the other hand, it could be argued that the absence of such complex enterprise applications and IT infrastructure even facilitates cloud service integration (Khanapurkar, 2011).

According to (Cisco, 2010), reducing costs and business agility are typical business factors for enterprise migration to clouds. In this connection, cloud computing can provide significant cost savings due to the increased utilization resulting from the pooling of resources and the standardisation and automation required for cloud services. Another business driver for cloud migration is that it

enables rapid delivery of IT services, which increases business efficiency. This increased IT efficiency translates to overall business efficiency, with the potential to unleash new innovations opportunities. Furthermore, from an operational stance, manageability, performance, and scalability are typical business reasons why enterprises consider cloud computing. For instance, by delegating the management of infrastructure and software platforms to a cloud service provider, customers can transfer operational responsibilities to service providers.

2.9.7 Barriers to Enterprise Cloud Migration

Migrating enterprise IT systems and applications to the cloud is a complex process that requires careful planning and deliberation. Cloud migration issues, such as, data security gaps, interoperability and portability challenges, disparity in cloud APIs, the dreaded 'vendor lock-in' situation, problems with SLAs and other legal uncertainties, which altogether constitute the actual migration and integration task, can create significant obstacles for enterprise cloud migration projects. Moreover, amongst the issues above, vendor lock-in and security as reported by Sahandi et al. (2013) are core drawbacks to enterprise cloud adoption in the UK.

Security issues are related to the location of data, its accessibility to third parties and its sustainability to losses. For most enterprises, intellectual property (IP) and knowledge in the data they own is their greatest asset. This is understandable seeing as they are reluctant in putting and hosting such corporate data in the cloud environment where they do not maintain absolute control over. Another constraint in this respect comes from the data protection and privacy laws enforced by different governments. Such laws call for strict geo-location restriction of data hosting and movement (in and out of cloud environment). Another barrier is the problem of how to verify if the SLAs is honoured, for instance in the case of data breaches, violations etc, and how can such violations be proved for possible claims and settlements? Of even more significance is the issue of the disparity in cloud APIs provided by different cloud vendors to the end users. Such disparity results in vendor lock-in situations where a cloud consumer is unable to migrate their cloud deployment to another cloud provider because of interface incompatibilities between the two (Harsh et al. 2012). Additional problems may be related to the obstacles faced by enterprises while integrating cloud computing to the business architecture. Besides, integration of cloud computing may indeed require special knowledge and skills – this may lead up to higher costs associated with attraction of specialists.

While these challenges are legitimate impediments to enterprise cloud adoption and migration, it is important for organisations migrating to the cloud environment, whether from in-house data centres or from one cloud to another, to understand these considerations upfront and temper any exorbitant expectations. It is also very important to underline that with any migration to cloud, there are one-time costs involved as well as resistance to change among the staff members (cultural and socio-political impedance). While these costs and factors are outside the scope of this thesis, it is

recommended that organisations take these issues into considerations when initiating a cloud migration project. For example, businesses can begin by building organisational support via evangelising and training. Another strategy that will help organisations simplify such migration challenges is the need to craft a well-thought-out migration strategy.

2.10 Chapter Summary

Vendor lock-in affects the application and data migration in cloud computing. Therefore, by improving the interoperability, portability, integration and standards of cloud applications (i.e., the degree of effectiveness and efficiency of a migration) organisations can reduce the risks of vendor lock-in. This chapter clarifies some decisions made in this research by analysing reports of real experiences of application, infrastructure, data and technology migration in scenarios that involve migration related or not related to the cloud. In addition, our analysis of relevant literature considers recent studies that provide guidelines for migration to the cloud. Overall, in this chapter we have discussed pertinent cloud computing adoption and migration challenges, from a business purview, to illustrate and describe consumer (interoperability and portability) requirements in using cloud computing SaaS service offerings. The selected literature sources and arguments deliberated in herein are based on high-level usage scenarios and a description of core concepts identified as relevant for all cloud computing service models, but specifically aimed at SaaS user-roles and migration scenarios. For example, the comprehensive analyses of the heterogeneity roots within the cloud environment reflect on the role and importance of the relationship between interoperability, portability, integration and security etc. These areas have been comprehensively discussed as they are crucial to understanding the work presented in the rest of this thesis. However, the focus of this thesis is on investigating mitigating approaches for tackling potential risks of vendor lock-in at SaaS layer of the cloud computing stack. Therefore, the scenarios presented here serves the purpose of highlighting some but certainly not all the cases where interoperability, portability, and security are important issues in the cloud computing environment.

Migration to the cloud environment is not without pitfalls, and is fraught with vendor lock-in challenges which may affect the overall migration process. Therefore, to summarise, in the next two chapters, author narrows the discussions presented herein to focus specifically on the socio-technical aspects of vendor lock-in and how such intricate areas affect enterprise cloud migration decisions (i.e. Chapter 3). Such discussions are further substantiated with empirical data analysis (i.e. Chapter 4). We use data produced in both chapters to build a cloud migration decision framework for the effort to avoid vendor lock-in risks when implementing or migrating between cloud-based solutions and vendors within existing enterprise IT environment. Note each of the two chapters starts with its own short background that clarifies additional concepts used only in the chapter.

Chapter Three

3. Vendor Lock-in

This chapter reviews key concepts and terminology needed for understanding the complexity of the vendor lock-in problem being investigated in this thesis. Firstly, we present aspects of cloud computing that contribute to vendor lock-in and briefly introduce existing results from cloud-related areas of computer science that contributes to understanding and tackling vendor lock-in (Section 3.1). Next, we explore the literature on vendor lock-in in cloud computing to identify its consequences, causes and current challenges faced by enterprise migrating to cloud-based services (Section 3.2). Note, the exploration of related literature has been based on a systematic review protocol (*see **Appendix 1***). Then, we propose taxonomy of cloud lock-in perspectives based on reports of real experiences on migration to understand the overall cloud SaaS migration process (Section 3.3). Finally, we narrow down to our perspective on cloud lock-in, to three main perspectives which takes the use of sound techniques from IS research discipline and cloud-related literature into consideration to improve the portability, security, and interoperability of cloud (and on-premise) applications in hybrid environments (Section 3.4 – 3.8). Collectively, the discussions presented within sub-sections of this chapter accordingly enables both academia and IT practitioners in the cloud computing community to get an overarching view of the process of combating application and data migration, and security challenges in the cloud.

3.1 Overview

The vendor lock-in problem in cloud computing is the situation where customers are dependent (i.e. locked-in) on a single cloud provider technology implementation and cannot easily move in the future to a different vendor without substantial costs, legal constraints, or technical incompatibilities (Michael et al. 2010). To substantiate further from the lenses of a software developer, the lock-in situation is evident in that applications developed for specific cloud platforms (e.g. Amazon EC2, Microsoft Azure), cannot easily be migrated to other cloud platforms and users become vulnerable to any changes made by their providers (Sitaram and Manjunath, 2012). The lock-in issue arises when a company, for instance, decides to change cloud providers (or perhaps integrate services from different providers), but is unable to move applications or data across different cloud services because the semantics of resources and services of cloud providers do not match with each other. This heterogeneity of cloud semantics (Loutas et al. 2010) and cloud Application Program Interfaces (APIs) creates technical incompatibility which in turn leads to interoperability and portability challenges (Rodero et al. 2010). This makes interoperation, collaboration, portability and manageability of data and services a very complex and elusive task. For these reasons, it becomes important from the view point of the business to retain the flexibility to change providers per business concerns or even keep in-house some of the components that are less mission-critical due to security

related risks. Interoperability and portability among cloud providers can avoid the problem of vendor lock-in. It is the way toward a more competitive market for cloud providers and customers.

3.1.1 What is Lock-in?

Vendor lock-in or being tied to a specific vendor deployment environment is what hinders many enterprise IT consumers to migrate to the cloud. The vendor lock-in situation challenges cost reduction and portability across multiple vendors. Due to the clouds nature of offering IT services to enterprise consumers using a pay-as-you-go billing policy, which ties the operating expenditure to the providers' offer. In turn, selecting the best offer may dictate a shift from one provider to another; incurring a switching cost, as well as the need to partially or completely redevelop the application, making this shift even more difficult and costly (Harsh et al. 2012), in the first place. At the core of this lock-in situation, we can identify a need for businesses to be able to easily migrate from one cloud provider to another, if perhaps they discover problems or if their estimates predict future issues.

An IDC executive insight research confirmed, while cloud providers are eager to migrate customers onto their platform and readily provide tools to do so, customers have voiced their concerns about the inconvenience of moving applications and data from one cloud to another (Bozman, 2010). Cloud vendors offer enterprises proprietary cloud-based services that have different specifications from one vendor to another. Vendor lock-in problem has been identified as one of the most widespread and crosscutting problems related with cloud computing adoption (Stravoskoufos et al. 2013). The risks posed by vendor lock-in can inhibit organizations from switching cloud providers (Armbrust et al. 2009; Pearson and Benameur, 2010). Razavian et al. (2013) conducted an analysis on how vendor lock-in prevents enterprises from migrating towards cloud storage. The outcome of their study proposed a solution that uses erasure coding as a method of distribution, to distribute redundant data across multiple cloud providers to increase the probability of access to data. Whereas, Bhavya et al (2013) discuss challenges concerning vendor lock-in problem in cloud computing and presents new ways of overcoming them. In addition, they addressed user concerns in portability and interoperability in the migration of cloud services providing security. With respect to cloud computing, vendor lock-in is the direct result of the current difference between the individual vendor paradigms based on non-compatible underlying technologies, and implicit lack of interoperability. Interoperability and portability are essential qualities that affect the cloud under different perspectives (Petcu and Vasilakos, 2014; Mell and Grance, 2009), due to the risk of vendor lock-in. Avoiding vendor lock-in or minimising its impact is consistent with ensuring interoperability and portability across cloud computing systems and services.

Cloud computing services have made it easier for organizations to rapidly deploy and de-provision IT applications on-demand as business needs evolve. When an enterprise system or application is moved to the cloud, it must use the APIs of a cloud service provider. There are APIs for

each of the types of cloud services listed in Section 2.4.1. But these APIs are generally not interoperable. So, although the situation may change in the future, an enterprise architect or decision maker, application developer etc. must make an informed choice to select the vendor that both best suits their business needs and allows the organisation to have the greatest flexibility (Sosinky, 2011). Issues associated with vendor lock-in have been identified and discussed below.

3.1.2 Cloud Lock-in Problems

Lock-in creates impediments for enterprises to easily switch cloud computing providers. The danger this brings to the cloud computing industry is that switching costs will rise, and this will reduce IT flexibility and increase the cost of application migration. This is problematic for organisations as frequent migrations (whether from on-premise to cloud or within the cloud) are necessary in the still nascent but dynamic, competitive, and constantly evolving cloud computing industry. In turn, this makes cloud migration a costly, time consuming, complex, and error-prone process for enterprises to handle. The core problems of cloud lock-in have been identified and discussed below.

A. Lack of Interoperability Makes It Difficult to Consolidate Enterprise IT Systems in the Cloud

Enabling cloud infrastructure to evolve into a transparent platform while preserving integrity raises interoperability issues (Armbrust et al. 2010). Interoperability of information between multiple clouds is a critical enabler for broad adoption of cloud computing by enterprises (Pooyan et al. 2013). Interoperability in cloud computing has many definitions from different points of view, and is often misused to include the term portability, as evident in (Wang, 2013). To clearly enunciate for the sake of clarity, we employ the distinction made by the National Institute for Standards and Technology (NIST) between interoperability and portability by defining interoperability as, "the ability of cloud computing services, from different providers, and other applications or platforms that are not cloud dependent to seamlessly exchange assets (Sheth and Ranabahu, 2010)." In a cloud environment, consumers favour greater interoperability as it allows them to customize their own solutions by purchasing "best of breed" services from multiple cloud providers and to move easily between providers. Governments, on the other hand, also favour interoperability as a way of driving competition and increasing resilience of the cloud system especially where the market consists of only a few providers (WEF, 2011). Further, another interoperability advantage for consumers (besides avoiding vendor lock-in risks) is that they would be able to compare and choose between providers. Also, the use of multiple clouds or hybrid clouds becomes possible when interoperability is supported. However, interoperability concerns arise in different situations. For example, interoperability between cloud layers needs standardized APIs to allow higher cloud layers to link, exchange and interact to a range of services provided at the lower layers e.g. platform implementations to uniformly link to Infrastructure-as-a-Service (IaaS) offerings. Although it is worth underlining that various cloud service models might have different requirements regarding interoperability. Therefore, fostering

cloud interoperability is multi-faceted and is likely to extend to a broad range of ecosystem players, including providers of connectivity and application developers. To this end, we suggest standards bodies, industry players, academia, practitioners etc. should pursue the evolution of cloud offerings with the goal of facilitating interoperability among multiple clouds. In fact, this will undeniably accelerate the maturity and growth of the overall cloud ecosystem.

B. Lack of Portability Hinders Enterprises from Migrating

Portability defines the ease of ability to which application components are moved and reused elsewhere regardless of provider, platform, operating system, infrastructure, location, storage, data format, or API's. Cloud portability is defined as the ability to migrate a cloud-deployed asset to a different provider (Mell and Grance, 2009), and it is a direct benefit of overcoming vendor lock-in. Petcu in (Wang, 2013) identified the following as the main kinds of cloud computing portability to consider; data portability, application portability, and platform portability. Whereas in (Dillion et al. 2010), they distinguish the different levels of portability within the cloud service models: IaaS portability involves the migration of virtual machines, whereas Platform-as-a-Service (PaaS) portability is the migration of code and data. While SaaS portability is the migration of data and content (JISC Legal, 2011). Data being an organization's most critical, ubiquitous and essential business asset, it is vital that any enterprise data migration be carried out without any disruption to data availability. Considering the different attributes of each cloud service model, the idea of data portability will depend on the model adopted. For this reason, organizations are interested to know whether they can move their data and applications across multiple cloud environments at low and minimal costs. Portability is the key aspect to consider when selecting cloud providers as it can both help prevent vendor lock-in, and deliver business benefits. This means allowing identical cloud deployments to occur in different cloud provider solutions (Lewis, 2012). Portability in cloud computing is a desirable expectation by organizations as they mitigate cloud outages and supports pursuing new business opportunities (e.g. better price, better service quality etc.). Cloud Security Alliance (CSA, 2011) believes that the first and foremost step required to ensure cloud service portability is the standardization of the data formats used by service providers. In contrast, industry stakeholders are concerned that an excessive focus on ensuring portability in cloud computing will limit the incentive to innovate by making it harder to differentiate between different architectures and offerings (WEF, 2011). While on the other, organizations wish to have the capability to move applications across platforms and data across applications, but they are hindered due to the disparity in cloud APIs provided by different vendors. Nevertheless, organizations planning to adopt cloud computing services must realize that moving business IT applications and (sensitive) data beyond the corporate firewall into the cloud environment is a form of outsourcing. And the golden rule of outsourcing is to understand up-front and plan for how to exit the contract. In this case, portability

should therefore be a key criterion of any organizations strategy to move into cloud services, allowing for a viable exit strategy to be developed.

C. Lack of Standards Creates Barriers to Cloud Entry

Standards are necessary to consolidate efforts in a technology domain and to enable interoperability and portability. The fields of standardization can be security, interoperability and portability, but the latter two are in the focus despite the importance of security. Standards are regularly proposed to mitigate vendor lock-in. However, in (Govindarajan and Lakshmanan, 2010), they argue that many cloud providers are concerned with the loss of customers that may come with standardization initiatives and do not regard this solution favourable. In agreement with (Wang, 2012), we suggest that standards shared among cloud providers do not need to be identical (i.e. in terms of differentiation advantage), although the greater the uniformity between them, the easier it will be to evaluate potential liabilities in choosing among the services offered by different providers. Moreover, any inconsistency could hinder a user's ability to move data or applications between providers, and might also limit an organization's ability to draw on the resources of multiple providers. Standardization strives to support applications by different service vendors to interoperate with one another, exchange traffic, and cooperatively interact with data as well as protocols for joint coordination and control (Ahronovitz, et al. 2010). Per (Machado et al. 2010), cloud users would particularly welcome standards that address workload migration and data migration use cases because such standards would mitigate vendor lock-in concerns. This requires virtual-machine (VM) image file formats and APIs for cloud storage (Yoo, 2010). In the absence of standards for cloud APIs and data models, companies willing to outsource and combine range of services from different cloud providers to achieve maximum efficiency will have trouble when trying to get their in- house (legacy) systems to interact with the cloud provider's system. Likewise, the lack of standardization may also bring disadvantages, when migration, integration, or exchange of resources is required. The main negative aspect in this case would be the necessity of factoring applications to comply with other cloud APIs, which can possibly lead to higher costs, project delays, and other related risks. Thus, opposing agility, efficiency, and low cost that often comes with utilizing cloud-based services (Cisco, 2010). The impact caused by lock-in problem due to lack of standards is what enterprises should be wary about when considering migration to cloud computing.

D. Technical Barriers

1) Integration Challenges: According to Buyya et al. (2010), cloud adoption will be hampered if there is not a good way to integrate data and applications across clouds. In (Stravoskoufos et al. 2013), it is argued that the cost and complexity of developing and maintaining integrations between heterogeneous platforms with disparate interfaces and protocols can quickly erase the economic and efficiency gains the cloud delivers. Moreover, a survey by (ISACA, 2012) of

business managers around the world on their experiences with cloud applications, revealed that companies have abandoned the use of roughly one departmental cloud application a year due to integration problems. It is anticipated that standardization of API's will significantly help to resolve this issue. However, initiatives by multiple standard bodies, forum and consortiums could indirectly lead to the possibility of multiple standards emerging with possible lack of consensus – thereby deteriorating the problem even further. But as advised by (Kavis, 2014), it is important for standard bodies, vendors, and users to sit together, discuss and arrive at a consensus on the standards and API's in different areas.

2) Data Portability Issues: Ensuring data portability within the cloud is a major challenge for enterprises due to the large number of competing vendors for data storage and retrieval (Linthicum, 2010). Suppose an enterprise uses SaaS product for Customer Relationship Management (CRM), and over time the terms of use of the cloud service become less attractive compared to other SaaS providers or perhaps with the use of an in-house CRM solution. If the business decides to change providers due to unacceptable increase in cost at contract renewal time, breached SLA etc. The key issue of concern for the organizations in this case is basically how easy will it be to move their data to another CRM solution or back in-house? In many cases, it will be very difficult because the data structure for cloud computing is not yet standardized. Quite often it is designed to fit a form of application processing logic, thus a significant amount of transformation is needed to produce data that can be handled by a different product. In this case, lock-in can be a deliberate strategy as it benefits vendors because it reduces the bargaining power for the enterprise and increases that of the vendors by gaining them a competitive advantage. From a portability perspective, it becomes critical that organization data is sharable between providers since without the ability to port data it would become simply impossible to switch cloud service providers at all (Parameswaran and Chaddha, 2013).

3.1.3 Societal Impact of Cloud Lock-in

- Oligopoly Market with reduced Competition

The adoption of cloud computing by organizations, however, does not imply that all the challenges in using the cloud have been well understood by most enterprises. Vendor lock-in has been studied in economics research communities, for example by Cowan (1991). Cowan identifies two sources of vendor lock-in: 1) uncertainty of selecting an unknown technology and 2) the learning curve of a technology. The current cloud computing landscape consists of many heterogeneous service offerings, from different cloud providers. Bear in mind that, these differences in offerings result in application architectures dictated by service provider specific features, ultimately resulting in non-portable, vendor-locked applications. As an increasing number of cloud providers start to provide cloud

computing services, they form a competition market to compete for consumers of these services (Feng et al. 2013).

By observing the current advancement in the cloud market, one can induce the overall cause of vendor lock-in. With the growing number of cloud computing service providers globally – cloud storage and compute service providers. As companies opt in to use these offerings, they become tied to a specific cloud provider technology, which cannot be easily switched or replaced without significant switching cost. Consequently, the lock-in situation exists since the cost of switching from one cloud vendor's operating environment to another is too costly that the customer is effectively unable to migrate from that vendor's offerings (Pierce, 2012). That results in a huge reduction in the benefit otherwise realized by switching cloud vendors. In some cases, the migration cost can even eliminate any benefits of moving, in the first place.

Whether cloud computing services provided by different vendors can interoperate, or whether they have a common interface, has become a major problem to be solved (Wang et al., 2012). Cloud solutions used by enterprise, in many cases depend on certain provider specific features or services. In migrating to the cloud, enterprises, application developers, as well as hardware/software provider's alike face the challenge of balancing these dependencies to avoid vendor lock-in. Therefore, developing applications to leverage one cloud provider's offerings can lead to lock-in with one vendor's solution and with limited or no competition. Vendor neutrality in this case is often best achieved by utilizing industry or open standards, but these standards are currently evolving for several layers of the cloud computing stack (as will be discussed later in this report).

- Large Switching Costs

Against the background in the preceding section, it can be drawn that the need for multiple vendor clouds to work together seamlessly (i.e. cloud interoperability) and support data portability smoothly is important to minimise the societal impact of lock-in. Cloud consumers require the ability to change cloud providers easily and should be free to choose the one that better serves their business needs in terms of quality and/or cost. This will also include the ability to use an organization's own existing data resources seamlessly. Previous research, in most models of consumer choice regarding switching costs due to technological lock-in, has identified several technical features of products that result in large switching costs and not surprisingly these features can be found in cloud computing systems. Existing cloud computing systems and services display what David (1975 & 1985) has called "*technical interrelatedness*": i.e. (1) generating output requires a multi-component system, and (2) the collection of components must be technically compatible to work together and achieve efficiency in system performance. It is easy to illustrate the two aspects of technical interrelatedness using cloud computing systems. First, they are multi-component. Second, compatibility plays an obvious role in enterprise migration decisions.

The former simply means cloud computing systems are composed of a variety of components ranging from central processor unit(s), input-output devices, communication terminals, memory/storage devices, system software, and application software etc. In a cloud environment, these components are often supplied by the same vendor. But to accomplish the virtual deployment and management, current cloud architecture requires cloud consumers (i.e. developers or end-users) to manipulate an API that is implemented by the cloud provider. However, since cloud APIs are not yet standardized, in effect this leads to proliferation of proprietary technology solutions and cloud applications. In the latter, technical incompatibilities can occur on many levels within the cloud computing technology stack, ranging from:

- system software not being unable to work with hardware architectures other than the one on which it is written unless the software is altered–also known as application refactoring;
- higher level software applications being incompatible with cloud system software implementations available on the new operating environments or platforms; and
- high level software optimized for implementation on one machine architecture may lose significant performance if implemented on another cloud provider's system.

Taking into consideration all these levels of technical interrelatedness within the cloud ecosystem, it is observed that most switching costs because of the lock-in situation will result from migrating from one incompatible vendor-specific technology solution or platform (i.e. operating environment) to another, not from mere changing providers per se. However, as explained by (Toivonen, 2013), vendors support incompatible cloud platforms because it is a way to differentiate services and functionality. In terms of differentiation advantage, Harmer et al. (2009) affirms by adding that, it is the interest of cloud providers to have their own APIs as this simplifies their development task, soothing their business model and implementation. Further, differentiation enables cloud providers to implement powerful features, innovate and enhance their services. In addition, it gives competitive advantage to industry giants (such as Google, Amazon, Microsoft, IBM etc.) already dominant in the cloud market place. For these reasons, lock-in is exacerbated as a major obstacle to enterprise cloud adoption and migration, considering the following factors:

- it creates monopolies for vendors with certain customers and as such limits the pressure to innovate
- it is a great drawback to customers, who jeopardize the freedom to evolve their software and become vulnerable to price increases, reliability problems, or the possibility of their vendors going out of business
- it may provide incumbent vendors with market power and may also influence customer and vendor choices among alternative cloud technologies or solutions.

Therefore, it should be underlined that selecting a cloud solution that is built on proprietary formats means that businesses can face a lock-in situation which will make it more difficult for them if they change service provider at some point in the future; either because they want to bring processes back into their premises or maybe they want to select another service provider. And quite clearly, this may kill the cloud ecosystem by limiting cloud service choice amongst consumers.

- Bottleneck for Cloud Migration Projects

The early stage of cloud technology has resulted in a variety of implementations and solutions where each vendor defines their own interfaces and approaches for similar products and services (Chow et al., 2009). This lead cloud applications, data and services to be tightly coupled to the proprietary cloud technology they were designed for – also known as lock-in. This lock-in effect refers to the dependency created between the cloud consumer and cloud provider, since the cloud consumer deploys their software on the provider's platform (Satzger et al., 2013). This dependency is created due to the heterogeneity of the services offered by different cloud providers. In this situation, a user is stuck or locked-in, with their current provider because of the complications of switching to a new vendor. In other words, the use of a cloud solution could potentially require buying into the specific protocols, standards, and tools of the provider. Essentially, this would make future migration costly and difficult.

A. Business Challenges

From a business perspective, many cloud providers seek to make their offerings to consumers as proprietary as possible to facilitate cloud vendor lock-in on the product, as well as at the contract level. There is more than one way to get locked into a cloud vendor's system; an often-overlooked method is through a contract. To substantiate further, a joint survey by Cloud Security Alliance (CSA) (CSA, 2011) and Information Systems Audit and Control Association (ISACA, 2012) identified exit strategies, contract lock-in and data ownership as core enterprise concerns. While another study conducted by Constellation Research Group found that many cloud contracts come with all the rigour and due diligence of on-premise licensed software. In this connection, per (Wang, 2012), there are three reasons why consumers face vendor lock-in; have limited rights and controls for users, ambiguous and ultimately expensive switching costs and vendor complacency. Vendors use the key selling point of cloud services (i.e. benefits of moving from capital expenditure to operational expenditure model) to significantly reduce the upfront costs for companies looking to implement new IT services and software. However, to minimise the risk of customer churn eroding their margins, vendors seek to create 'lock-in' through contractual terms, or through the physical holding of the customer's data. In this regard, there is an economic benefit to the vendor in the form of a regular revenue stream, but not so much of a business benefit to the consumers. From a commercial

perspective, this puts the vendor in a position of strength when it comes to renegotiating the commercial terms of the agreement. For this reason, it is crucial to carefully review the contract before signing. Considering the negative impact that these issues can have on a business operation, it is worth mentioning that when enterprises opt-in to use any cloud-based solution, the cloud service should at least provide tools to ensure the consumer can extract, access and interchange data if such a need arises.

B. Legal and Jurisdictional Challenges

A key advantage of utilizing enterprise cloud-based IT solutions from a cloud provider perspective is the flexibility and movement of data between servers that may be in various parts of the world. Further, data maintained in a cloud environment may contain personal, private or confidential information such as intellectual property (IP) etc. that requires proper safeguards to prevent disclosure, compromise or misuse. An enterprise or SME organization using cloud based IT services is likely to have processing performed in, and data moved between, different jurisdictions. Thus, this may place constraints on the processing that can be performed, on the movement of data, and on the degree of control that the organization has. Furthermore, it is observed that existing laws and governance are insufficient to keep pace with cloud computing service development (Avram, 2013). Thus, the potential for legal disputes is considerable. In addition, legislative and jurisdictional challenges may also arise due to the possibility of data centres located in areas with different jurisdiction. Bear in mind that many jurisdictions will have specific requirements and regulations regarding the location of data. Therefore, such requirements should be carefully considered by enterprises before a decision on adopting the cloud service model is made. We believe there are opportunities for lawmakers to come up with useful multi-jurisdictional regulations that will help in determining the applicable legislation in cases where data is in different jurisdictions. Policies need to be crafted around data interoperability related issues to ensure that data interchanged between cloud services is un-hindered, as most enterprise users are likely to use heterogeneous cloud service providers for their business needs. So, policy makers should focus on data ownership and control issues to ensure that enterprises continue to control the destiny of their data. It is important for cloud providers to put mechanisms in place to ensure that whatever enterprise data they put in the cloud service can be easily and securely taken out, for reasons such as integration with another cloud service, or a move to another cloud service vendor etc.

3.2 Vendor Lock-in and Enterprise Cloud Migration

From a historical viewpoint, many enterprise organizations fail when it comes to implementing new and transformational technologies. The following were identified as the main causes of failure: lack of understanding and interest in embracing new technologies; early rush into development mode without

proper understanding of architecture and design steps; and unrealistic expectations like too-aggressive due dates, too large of a scope and many other reasons (Kavis, 2014). A common misconception about cloud computing is the notion that migrating existing enterprise IT applications to the cloud, or replacing on-premise systems with cloud-based alternatives, is a simple solution that reduces cost. But this is usually the complete opposite. In fact, very few applications are good candidate to move to the cloud in their current architecture. The architecture of an application will affect how the application can be migrated to the cloud environment and sometimes whether it is suitable for migration. Cloud architectures, however, require loosely coupled application architectures – since it allows one to replace components, or change components, without having to make reflective changes to other components in the architecture/systems. This means enterprises can change their business systems as needed, with much more agility than if the architecture/systems were more tightly coupled (Linthicum, 2010). Therefore, in agreement with the recommendation by (Cisco, 2010), to identify business processes, application and data for operation in the cloud environment, it is mandatory to first develop and understand the technical, business and legal factors that might affect the migration process. Therefore, in the preceding sections, we have look at the societal impact of vendor lock-in on adoption of cloud computing services from a business and legal viewpoint.

3.2.1 Vendor Lock-in Risks and Challenges Related to Migrating and Operating in the Cloud

Viewing the cloud computing lock-in problem from a technical perspective may be too narrow to comprehensively analyse such a complex situation. Instead, complexity of cloud lock-in situations can originate from many other sources than the service (i.e. cloud or on-premise IT) system itself (Benedettini and Neely, 2012). In information system (IS) research, for example, such IT systems are considered as socio-technical systems involving technological components as well as people and the organizational environment interacting with it (Picot and Baumann 2009; Orlikowski 1992; Belfo 2012). We follow this research discipline and see cloud computing as a concept involving engineering as well as various management aspects. Thus, it needs a socio-technical approach to assess its characteristics and related lock-in risks from a holistic view. This calls for a need to contribute a review study that distils cloud migration approaches to understand the associated migration challenges, and what essential activities, tasks, and decisions are involved during the cloud-to-cloud migration or legacy-to-cloud SaaS modernisation/replacement. Thus, in this section we considered it useful to conduct a systematic review (in ***Appendix 1***) with the primary objectives: to firstly, summarise the empirical evidence of the approaches, benefits and limitations in the existing cloud migration research; secondly, to identify any gaps in current research tackling the vendor lock-in problem and cloud SaaS migration specifically, in order to suggest areas for further investigation and; thirdly, to provide a decision framework with guidelines as a prelude to further research activities to tackle the vendor lock-in risks in cloud computing environment (refer to ***Appendix 1***). To this end, the main objective of this sub-section is to obtain a holistic understanding of the vendor lock-in risks

associated with cloud migration research and investigate the influence such risk(s) have on enterprise decisions to adopt cloud-based SaaS solutions. Hence, the study presented here provides a concise yet relevant discussion and analysis of the current state of cloud computing migration and associated SaaS lock-in challenges with some fundamental guidelines that should be observed by organisations, entering a cloud computing service contract. However, considering most research in cloud computing migration (in industry and academia) generally starts with a literature review of some sort. The literature review is an essential approach to conceptualise research areas and synthesise prior research which directly contributes to a cumulative research culture (Webster and Watson, 2002). Therefore, unless the literature review is thorough and fair, it is of little scientific value (Keele, 2007); thus, our main rationale for undertaking a systematic review in this study.

Based on the results of the systematic literature review, **Figure 3.1** illustrates how several IT organisations are utilizing cloud service providers (CSP) with effective life-cycle management (i.e., in/exit/migration of services) to support critical/non-critical IT services (e.g., development and test applications). This utilization strategy is further exacerbated with the multitude of providers offering a wide variety of cloud services to consumers. This requires an effective strategy to engage CSP in enabling cloud solutions, shifting cloud services from one cloud service provider to another and discontinuing cloud services of CSPs when required. However, due to the absence of standards, cloud interoperability and portability, security (including data privacy and ownership), SLAs, and APIs are approached differently by each provider. Thus, switching and conversion (for application and data) costs is higher because of the incompatibilities between the current cloud products and offerings. This must be planned for in the contractual process as outlined in Step(s) 2 and 3 (in Section 6.3.2 – 6.3.3), in the business continuity program as outlined in Step 6 (in Section 6.3.6), and as part of the overall governance and exit strategy. However, since most cloud service providers use (flexible) contract terms and (negotiable) SLAs to convince potential customers to buy and use their services, even for mission-critical enterprise business applications. To mitigate and avoid specific risks of data and application lock-in at level 6 and 7 (i.e. switching and conversion costs) respectively, there needs to be an agreement on interchange data formats and structure to be defined in a manner appropriate for each specific software application area or market such as office suites, finance, healthcare etc.

Therefore, by evaluating different cloud offerings from the perspectives of associated elements presented in **Figure 3.**1, it can be said that standards for interoperability and portability will not only make it easier to develop and integrate cloud services with on-premise systems, but it will also make entering and exiting the cloud less risky, and hence attractive for enterprises by increasing their choice of providers. This also provides the ability for enterprises to adopt cloud and the ability to customize the cloud environment to fit their needs.

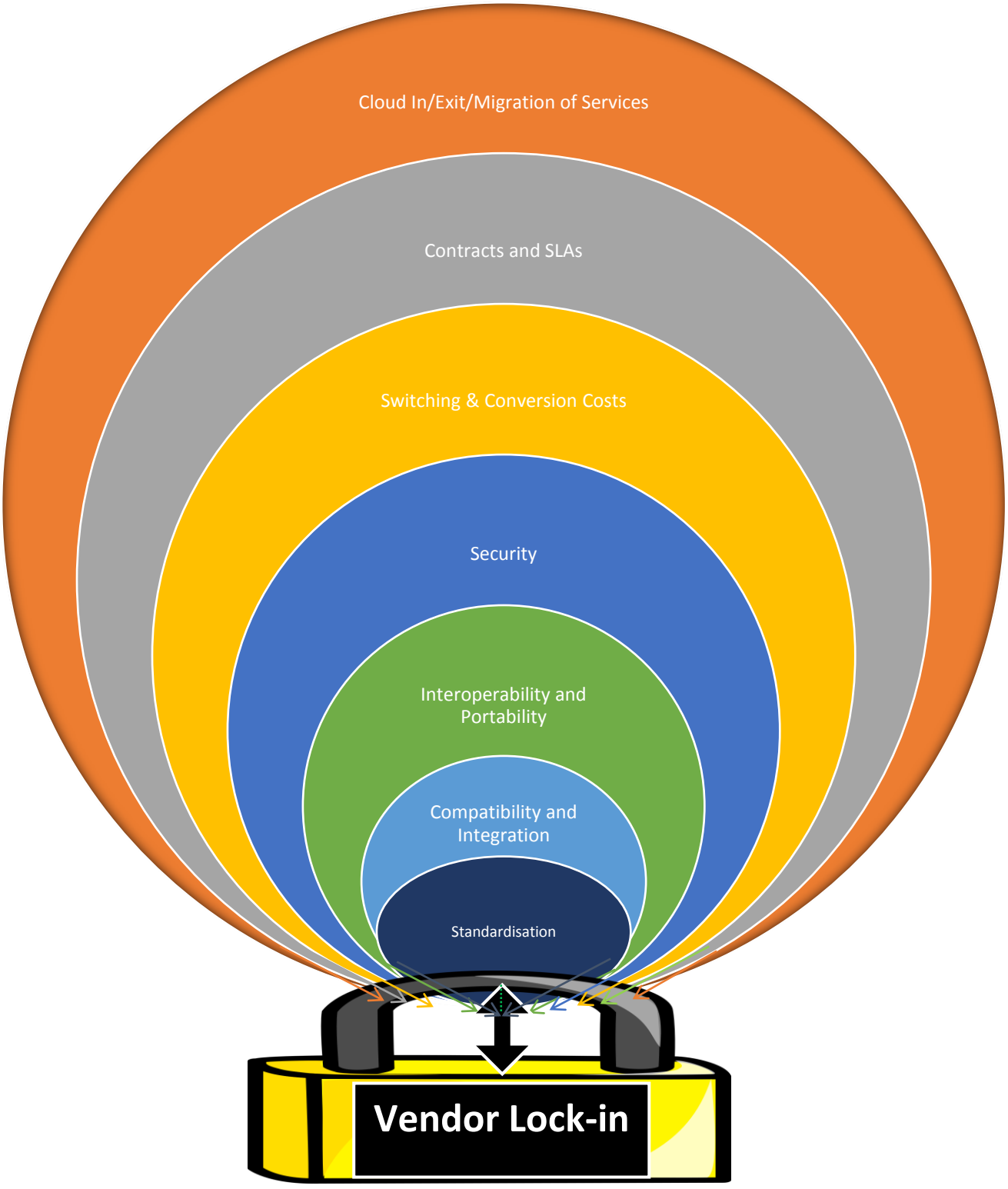


Figure 3.1- Relationship between Vendor Lock-in and associated elements

3.2.2 Taxonomy of Cloud Lock-in Perspectives

In **Figure 3.1**, a model encompassing the various elements (or triggers) of vendor lock-in risks in cloud computing is presented. The analysis of this multi-dimensional model shows that each element

can create different effect of lock-in on specific business processes operating in a cloud environment. With the intent to create a cloud lock-in model, both for studying proprietary lock-in challenges in the context of service migration, and for supporting decision making for enterprise cloud adoption. Authors' aim in this section is to consider the various risks and challenges of vendor lock-in presented in **Figure 3.1**, and organise them in hierarchical categories of perspectives, thus creating a cloud computing vendor lock-in taxonomy. But before doing so, it is important to make clear that for any given information processing system (whether in cloud or non-cloud environments) there are a few user categories - or more accurately, several *"roles*" - that have an interest in the system. Each role is interested in the same system, but their relative views of the system are different, they see different issues, they have different requirements, and they use different vocabularies (or languages) when describing the system. In this direction, rather than attempting to deal with the full complexity of cloud lock-in problem, author mainly attempts to recognize these different interests by defining different viewpoints of the lock-in problem in question. Each of these perspectives or viewpoints is chosen to reflect one set of inter-related consumer cloud lock-in concerns.

Across the three inter-related perspectives of vendor lock-in, organisations can use the proposed taxonomy to review their existing processes for cloud adoption and migration, data governance, and purchase policies to see if these support a strategy to achieve a high-level of flexibility and control to reduce the chance of being unavoidably locked into a single cloud provider offering. The aim of this taxonomy is to give both cloud service consumers (i.e. enterprises, end-users, developers etc.) and cloud service providers guidance in the provision and selection of cloud services, indicating how to mitigate the risk of being tied to a cloud service provider – due to the difficulty and costs of switching to use equivalent cloud service from other providers. The taxonomy of cloud vendor lock-in perspectives' partitions the challenges to address into three viewpoints; business, technical, and legal. Each of the viewpoints can be used as problem analysis technique as well as solution space of the relevant issues of the lock-in problem domain. The main structure of the taxonomy along with its top levels of classification is depicted in **Figure 3.2**. The illustration is not meant to be exhaustive but to give a precise yet accurate view of the broad problem of cloud lock-in from different perspectives.

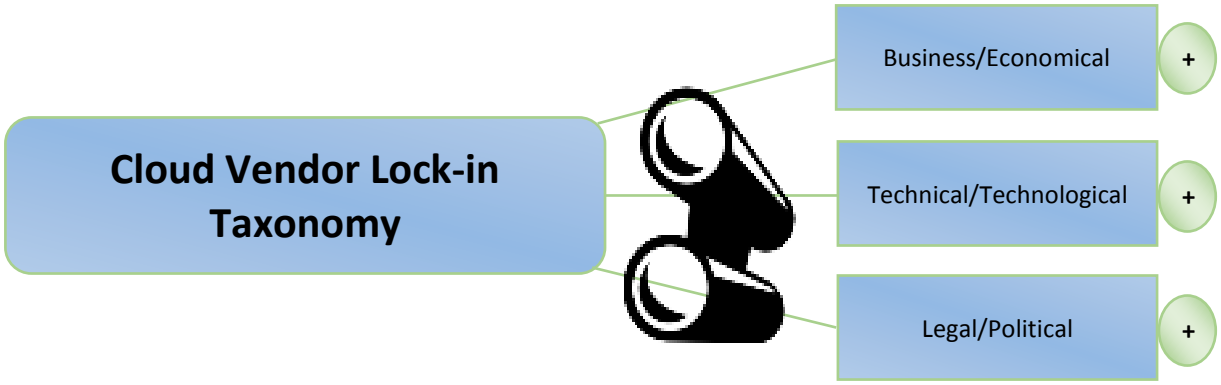


Figure 3.2- Perspectives for Categorising Vendor Lock-in Risks in Cloud Computing

Different projections on Vendor Lock-in: Top level overview of the viewpoints of cloud lock-in taxonomy, highlighting the three main perspectives to view the broad problem of vendor lock-in – related to business, technical and legal categories.

The three main perspectives of cloud vendor lock-in problem(s) are: business (or economics) perspective, technical (or technological) perspective, and legal (or political) perspective. Together they provide a complete picture of cloud computing vendor lock-in challenge. The concerns addressed in each of the perspective are precisely presented. For instance, the business dimension is subdivided into standards, interoperability, portability, and security. This organisation is depicted in *Figure 3.3*. The technical perspective includes constraints related to integration, compatibility, and APIs that are implementation-specific requirements or restrictions which may hinder Interconnectability and/or trigger lock-in situation in the cloud. The complete organisation of this scenario is presented in *Figure 3.4*. While the first two categories correspond to enterprise architecture requirements (for enabling interoperability and portability) of products and IT services based on standard interfaces to interact seamlessly without the need for a large amount of integration efforts. The legal or political perspective is split into four sub-categories (i.e. SLA compliance, contract termination, cloud migration strategies, metadata and data ownership) per the service life cycle and measures in which various aspects of cloud services offered and managed for a cloud service consumer can result in a lock-in situation. It is also noted that the lock-in risks in this dimension or perspective cover the complete information lifecycle (i.e., generation, use, transfer, transformation, storage, archiving, and destruction) inside the cloud providers' perimeter and in its immediate boundaries (or interfaces) to the consumers. The expansion of this categorisation is depicted in *Figure 3.5*.

3.2.3 Taxonomy of Cloud Computing Vendor Lock-in Risks

A clear perspective of the main risk factors that contribute to a lock-in situation in the cloud environment and how such risk(s) should be organised to ease decision making is the main step for having a comprehensive analysis of the status of cloud computing vendor lock-in challenges. To organise the complex and broad data related to cloud lock-in problems and to facilitate further studies

in this area, this section identifies the main problems (i.e. risks or challenges) of cloud lock-in, and group them into a model composed of eleven (11) categories namely; standards, portability, interoperability, security, integration, compatibility, APIs, data, contracts, SLA compliance, and cloud migration (in/out) strategies. Note that these elements are placed in a hierarchical order of significance to the broad lock-in problem, in general. These elements are significant considerations to the use of cloud services, and are also indicators to how component may trigger and/or intensify the risk of lock-in involved. The hierarchical categorisation approach assists in demonstrating how each element of vendor lock-in relates to several other components in the architecture of cloud computing. At a high level, the model establishes a common language (i.e. ontology) for easy understanding and communication of the capabilities and requirements which should be standardised in a cloud environment to facilitate open collaboration and interoperability amongst cloud providers – thereby avoiding the risk of a single provider lock-in. At a low level the model is further composed into taxonomy to support consumers cloud service selection and adoption strategy in terms of validating cloud provider's solutions to achieve architectural integrity of business solutions of an enterprises' cloud ecosystem.

Prior to presenting the proposed taxonomy, it should be pointed out first that the identification of elements and components of the categorisation used is based on the critical review of key literatures (in the preceding section and subsequent sections). This critical review followed the systematic approach proposed by Peng and Nune (2009 & 2012). Some of these studies include standards and proposal documents from academia and industry as well as independent quantitative and qualitative studies conducted by author. Apart from reviewing the studies in the preceding and sub-sequent sections, the systematic review also covered general computing, IT and information systems (IS) journals, conference proceedings, books, industrial white papers, and technical reports. The fundamental purpose was to identify broadly any possible factors and issues that might lead to or intensify potential risks of vendor lock-in. Through this extensive and critical literature review, author established and proposed a set of potential cloud lock-in risk factors using taxonomy. The taxonomy is explained and verified using case-examples from existing services of major cloud providers with an emphasis on the distinction made between services in software application programs (SaaS), platform (PaaS), and infrastructure (IaaS), which are commonly used within traditional enterprise computing or as the fundamental basis for cloud service classification. As would be seen in the subsequent section, different elements of lock-in encountered in each category is described below to aid readers' understand-ability of the overall complexity of cloud lock-in situation in more details. Each of these elements in the categorisation (or classification) model below, results in subdivisions highlighting the main risk factors of vendor lock-in that have been identified.

1) *Business Perspective:* It focuses on the needs of the consumers of a cloud product or service offering. It describes the business challenges of vendor lock-in in terms of answering what is

required of a cloud provider to meet customers' expectations to avoid over dependency on a product and the vendor. From a business perspective, avoiding vendor lock-in is requested by reasons varying from optimal service selection regarding utilisation, costs or profits, to technology (hardware or software) changes. The adoption of cloud computing is still hindered by the lack of proper technology (or technology maturity), knowledge (of use), transparency and trust issues. One of the problems spanning across these reasons is the low level of portability and interoperability of cloud applications and data storage services. The vendor lock-in challenge with respect to both low-level resource management and application level services is related also to the lack of world-wide adoption of standards or interfaces to leverage the dynamic landscape of cloud related offers. Portability and interoperability standards provide customers the ability to switch cloud providers without a lock-in to a provider. Moreover, data and applications in the cloud reside on systems consumers do not own and likely have only limited control over – which can result in loss of data and application security issues. Lack of interoperable and portable standards for different security policy or control, key management or data protection between providers may open undiscovered security gaps when moving to a new provider or platform. Hence, it becomes important to consider several items, for portable and interoperable security standards, to protect sensitive data being moved to or in the cloud. In this direction, author acknowledges that not all information used within a cloud system may qualify as confidential or fall under regulations requiring protection. Therefore, the security categories proposed in this case are based on information security lifecycle for protecting data in terms of confidentiality, availability and integrity (which can be applied not only to cloud environments, but any solution which requires basic interoperable and portable security integration). The complete organisation is depicted in **Figure 3.3**.

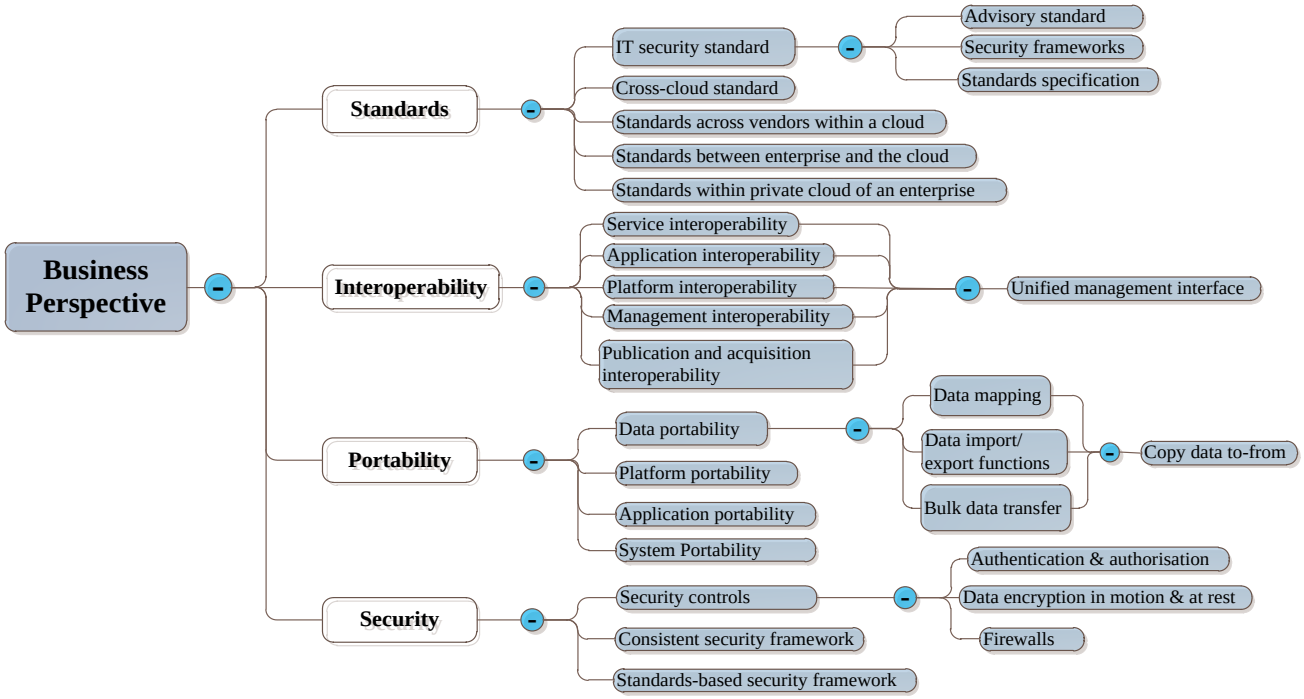


Figure 3.3- Vendor Lock-in Taxonomy – business perspective.

NB: Components from the business perspective of vendor lock-in are subdivided into 4 categories (i.e. standards, interoperability, portability and security). These elements are significant considerations to the use of cloud services, and are also indicators to how each component may trigger and/or intensify the risk of lock-in involved.

2) *Technical Perspective:* The technical dimension is subdivided into integration, compatibility and APIs. In this case, the classification proposed are based on technical constraints placed on consumer's ability to achieve seamless integration and compatibility with user, administrative and programming interfaces for using and controlling a cloud service. Since the interfaces and APIs of cloud services are not standardised; different providers use different APIs for what are otherwise comparable cloud services. These APIs expose the semantics (i.e. description of cloud services by its provider) and technologies (i.e. middleware and applications used to support a cloud service) used by a provider by providing the service management functionality. This implicit lack of standards (as pointed earlier) adoption by cloud providers is in fact a breeding ground for various types of heterogeneity (e.g. hardware and platform), because each cloud provider uses different technologies, protocols, and formats. This heterogeneity is a crucial problem as it gives rise to vendor lock-in situations in cloud computing. Thus, the need for a well-defined standard interface plays an important role towards achieving compatibility and manageability inside and between clouds. Then cloud service consumers can take advantage of seamlessly integrating different provider offerings, combine benefits of each cloud to build solutions that are coherent to their respective business goals. The complete categorisation of technical perspective of lock-in is presented in **Figure 3.4**.

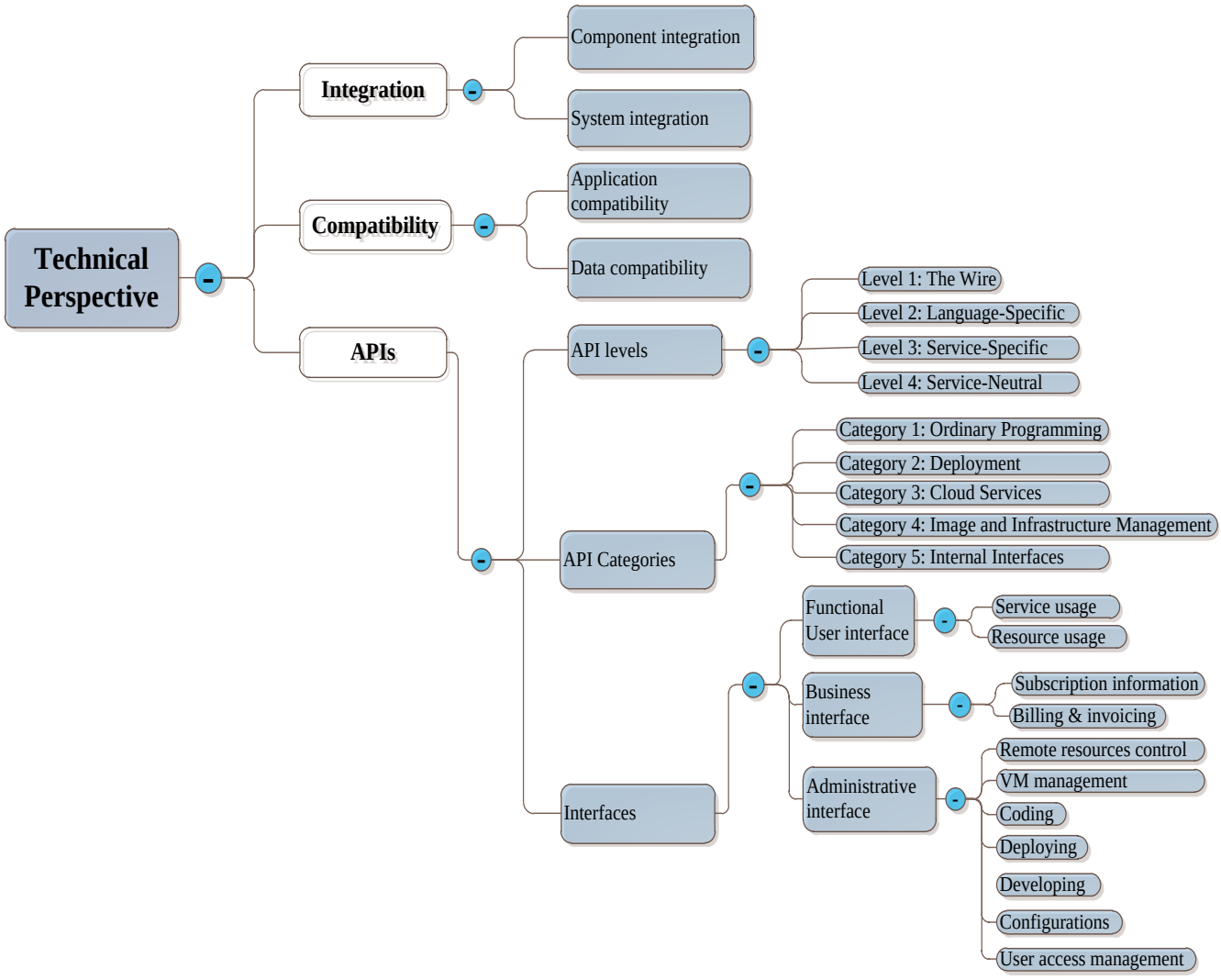


Figure 3.4- Vendor Lock-in Taxonomy – technical perspective

3) *Legal Perspective:* The need to avoid the risk(s) of cloud vendor lock-in from a legal perspective is to limit possible constraints on data, application and services per the locations or national laws, as well as grant customers the free will to avoid dependence on only one external provider. The categorisation in this dimension includes aspects related to contract and license issues, exit process or termination of use of a cloud service, judicial requirements and law (such as multiple data locations and privilege management). The legal perspective is split into four sub-categories (i.e. SLA compliance, contract termination and exit process, cloud migration strategies, metadata and data ownership) per the service life cycle and measures in which various aspects of cloud services offered and managed for a cloud service consumer can result in a lock-in situation. It is also noted that the lock-in risks in this scenario cover the complete information lifecycle (i.e., generation, use, transfer, transformation, storage, archiving, and destruction) inside the cloud providers' perimeter and in its immediate boundaries (or interfaces) to the consumers. Audit and monitoring are also important aspects

worth considering in the legal dimension, due to the requirements that a cloud provider should ensure to fulfil service agreements. For instance, the exit process or termination of the use of a cloud by a customer requires careful planning from an information security perspective. From a data security and storage perspective, it is important that once the customer has completed the termination process, none of the customer's data should remain with the provider. Thus, the exit process must allow customer to retrieve their data in a suitably secure form, backups must be retained for agreed periods before being eliminated and associated event logs and reporting data must be retained until the exit process is complete. Meanwhile, customers are advised to negotiate directly with their cloud service provider to ensure appropriate exit process provisions and assurances are included and adequately documented in their cloud SLA and contracts. The expansion of this categorisation is depicted in **Figure 3.5**.

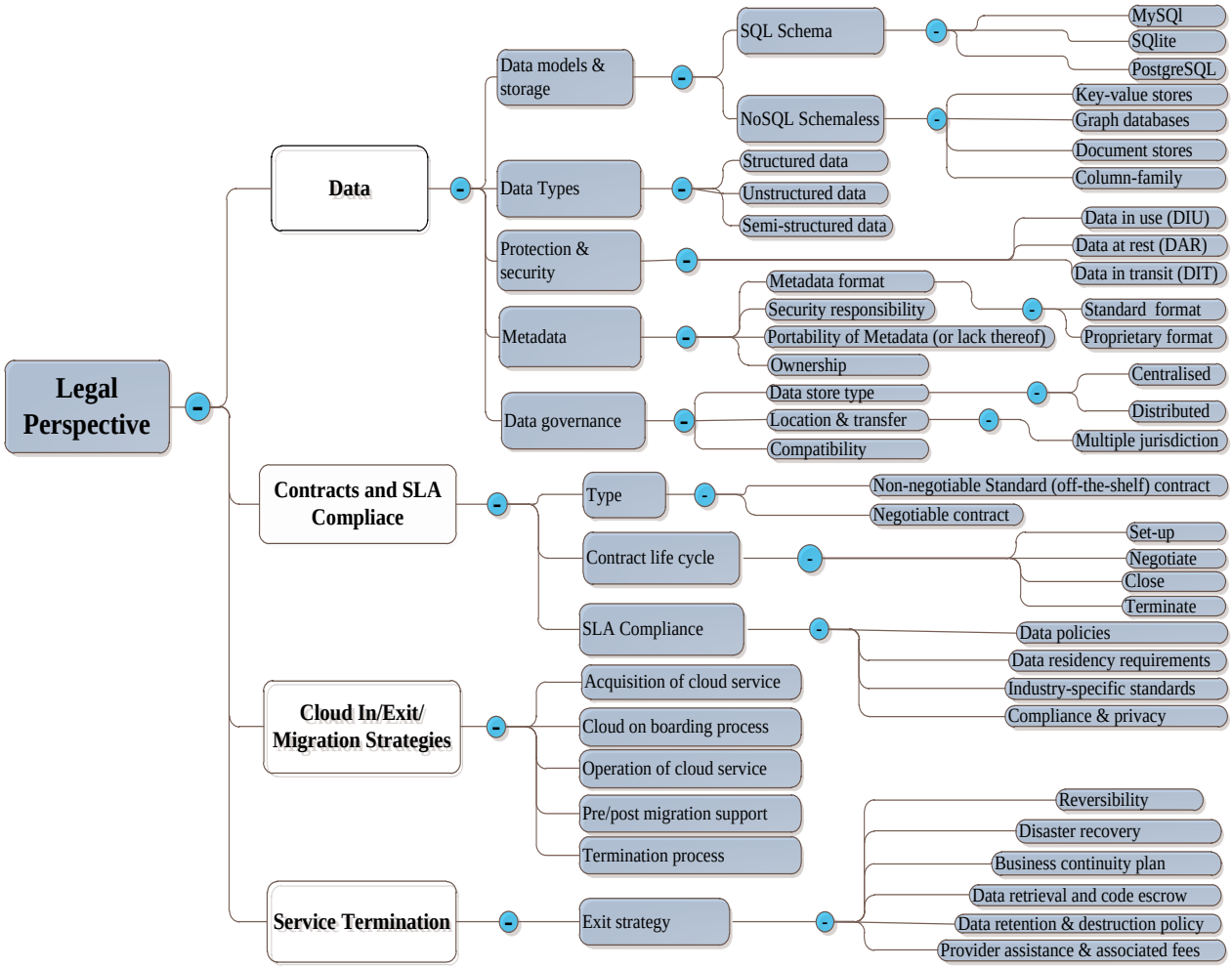
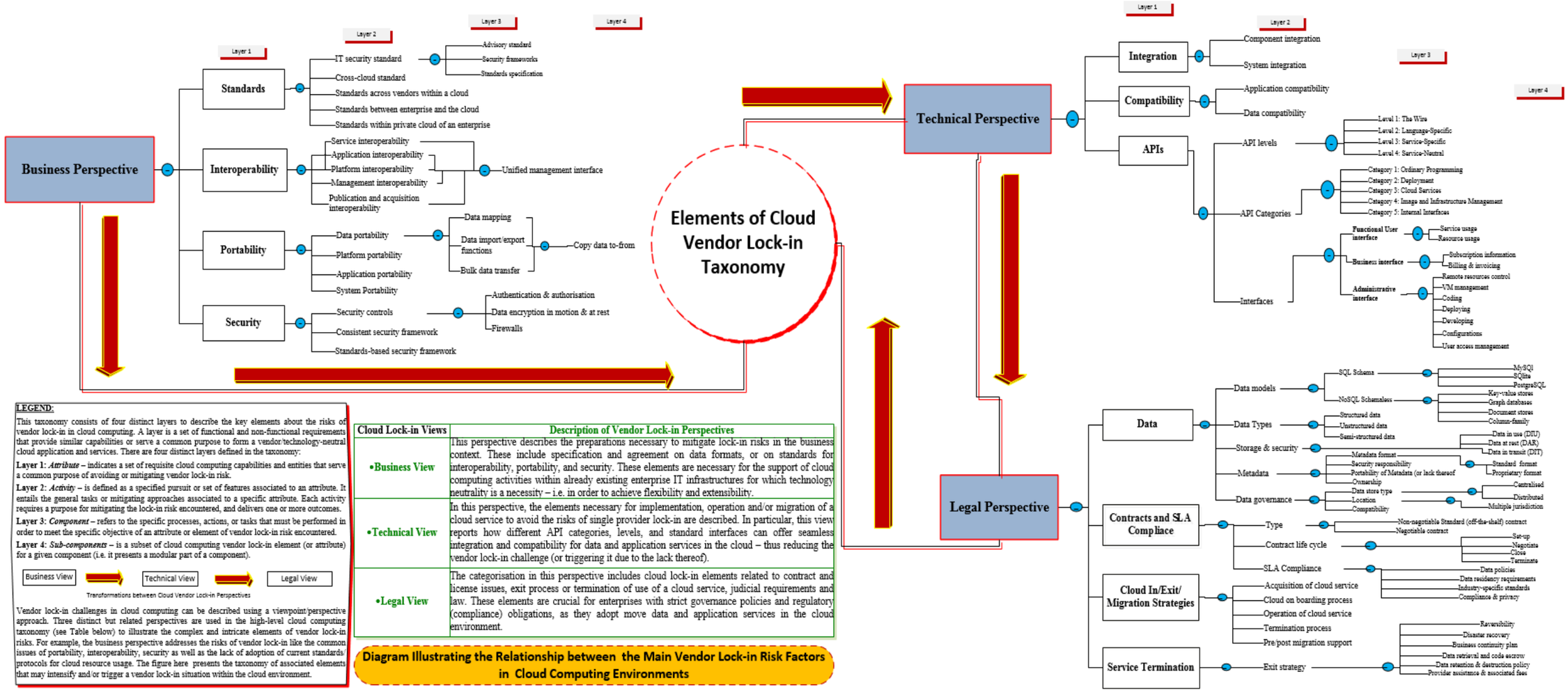


Figure 3.5- Vendor Lock-in Taxonomy – legal perspective

In **Figure 3.6** we present a high-level (combined) view of the proposed taxonomy. It shows the transformation between the different vendor lock-in perspectives. The different layers of the taxonomy are also made obvious within the high-level taxonomy of cloud lock-in risks. This high-level taxonomy of vendor lock-in risks identifies the key cloud computing interoperability, portability, API interface categories, as well as other relevant and intricate components of cloud systems that should be portable and interoperable. For example, standardisation of the interfaces between these components is the first step to achieving interoperability and portability – as it prevents being locked into any cloud or provider. In the expanded diagram, a layer represents a set of functional and non-functional requirements that provide similar capabilities or serve a similar purpose to support a vendor neutral (and technology-independent) sourcing strategy for cloud applications and services.

This high-level diagram includes both operational and architectural considerations that apply to multiple (i.e. cross-cutting) elements within the description of the cloud computing reference architecture (in *Section 2.4*), the adapted cloud computing taxonomy (in *Section 2.4.5*) and the proposed ontology for cloud SaaS application software architectures, in relation to how they trigger or intensify a cloud lock-in situation. These cross-cutting elements (*refer to Layer 1 in the diagram*) of vendor lock-in raise shared issues across roles, activities and components of a cloud computing system. For example, in a SaaS environment where a customer wants to move an application to a different cloud service provider (i.e. switch cloud SaaS providers), the cloud customer runs the risk of encountering a data lock-in if the (target/source) SaaS cloud provider does not use standard data interchange format(s) relevant to the target application domain. Moreover, the rest of the switching cost will include exporting, mapping and importing data into the new cloud service provider's SaaS application, and such cost is a function of how well the data models and formats of the two SaaS cloud service providers match up (i.e. compatibility).

Furthermore, changing between SaaS applications can also involve the cloud service customer adapting to a new service interface (which relates to the interoperability of the service). Again, interoperability here is a cross-cutting element of vendor lock-in and so is standards, portability, security etc. For example, security is a cross-cutting element of vendor lock-in because it applies to infrastructures, platform services, application software's, cloud service providers, cloud service customers, and cloud service brokers. These needs to be secured and remain interoperable, but how they maintain interoperability and security is different based on what is being secured and at what layer is security and interoperability required (see diagram). Securing infrastructure services is very different from securing application software services.



LEGEND:

This taxonomy consists of four distinct layers to describe the key elements about the risks of vendor lock-in in cloud computing. A layer is a set of functional and non-functional requirements that provide similar capabilities or serve a common purpose to form a vendor/technology-neutral cloud application and services. There are four distinct layers defined in the taxonomy:

Layer 1: ***Attribute*** **–** indicates a set of requisite cloud computing capabilities and entities that serve a common purpose of avoiding or mitigating vendor lock-in risk.

Layer 2: ***Activity*** **–** is defined as a specified pursuit or set of features associated to an attribute. It entails the general tasks or mitigating approaches associated to a specific attribute. Each activity requires a purpose for mitigating the lock-in risk encountered, and delivers one or more outcomes.

Layer 3: ***Component*** **–** refers to the specific processes, actions, or tasks that must be performed in order to meet the specific objective of an attribute or element of vendor lock-in risk encountered.

Layer 4: ***Sub-components*** **–** is a subset of cloud computing vendor lock-in element (or attribute) for a given component (i.e. it presents a modular part of a component).

Business View → Technical View → Legal View

Transformations between Cloud Vendor Lock-in Perspectives

Vendor lock-in challenges in cloud computing can be described using a viewpoint/perspective approach. Three distinct but related perspectives are used in the high-level cloud computing taxonomy (see Table below) to illustrate the complex and intricate elements of vendor lock-in risks. For example, the business perspective addresses the risks of vendor lock-in like the common issues of portability, interoperability, security as well as the lack of adoption of current standards/ protocols for cloud resource usage. The figure here presents the taxonomy of associated elements that may intensify and/or trigger a vendor lock-in situation within the cloud environment.

Cloud Lock-in Views	Description of Vendor Lock-in Perspectives
•Business View	This perspective describes the preparations necessary to mitigate lock-in risks in the business context. These include specification and agreement on data formats, or on standards for interoperability, portability, and security. These elements are necessary for the support of cloud computing activities within already existing enterprise IT infrastructures for which technology neutrality is a necessity – i.e. in order to achieve flexibility and extensibility.
•Technical View	In this perspective, the elements necessary for implementation, operation and/or migration of a cloud service to avoid the risks of single provider lock-in are described. In particular, this view reports how different API categories, levels, and standard interfaces can offer seamless integration and compatibility for data and application services in the cloud – thus reducing the vendor lock-in challenge (or triggering it due to the lack thereof).
•Legal View	The categorisation in this perspective includes cloud lock-in elements related to contract and license issues, exit process or termination of use of a cloud service, judicial requirements and law. These elements are crucial for enterprises with strict governance policies and regulatory (compliance) obligations, as they adopt move data and application services in the cloud environment.

Diagram Illustrating the Relationship between the Main Vendor Lock-in Risk Factors in Cloud Computing Environments

Figure 3.6- High-level Categorisation of Vendor Lock-in Risks in Cloud Computing

3.3 Service Models and Vendor Lock-in Risks

Currently, there is little on offer in the way of tools, procedures or standard data formats or service(s) interfaces that could guarantee data and service portability in the cloud computing environment. This makes it extremely difficult for a customer to switch cloud providers, or to move data and services from an in-house IT environment to the cloud. In effect, this potential dependency for service provision on a single cloud provider, may lead to organisational risks should the cloud provider, for instance, go out-of-business or bankrupt. Organisations considering adopting cloud computing models are concerned about the potential for lock in and the operational challenges that a storage migration (as an example) would require. Thus, it becomes important to understand that the extent and nature of lock-in varies per the cloud type:

- **SaaS Lock-in**: SaaS providers typically develop a custom application tailored to the needs of their target market. The consumer data of a SaaS product is typically stored in a custom database schema designed by the SaaS provider. However, if the provider does not offer readymade data export functionality, the customer will need to develop a program to extract their data and write it to a file ready for import to another provider. Where the customer has developed programs to interact with the provider's API directly (e.g. for integration with other applications), these will also need to be re-written to consider the new provider's API. SaaS suffers from data lock-in, contract lock-in and application lock-in risks.

- **PaaS Lock-in**: occurs at both the API layer and at the component level. At the API layer, PaaS lock-in occurs as different providers offer different APIs. PaaS lock-in happens at the component (i.e. runtime) layer as standard runtime environments are often heavily customised to operate safely in a specific cloud environment. PaaS suffers from framework lock-in and data lock-in (as in SaaS) but in this case the onus is completely on the customer to create compatible export routines and more importantly for the customers' developers to understand and consider these differences pointed out.

- **IaaS Lock-in**: varies depending on the specific infrastructure services consumed. Virtual machines (VMs) that can be moved to the cloud from (heterogeneous) data centres, and between vendors' IaaS clouds, are an asset for organisations. However, doing so requires cloud IaaS providers to support a standardised VM file format. Currently there is little in offer in terms of standardised file format for virtual machine images and VM management. While virtualisation can remove concerns about physical hardware, distinct differences exist between common hypervisors such as ZEN, VMware and others. For example, data lock-in is the obvious concern with IaaS storage services. IaaS storage provider offerings vary from simplistic key/value based data stores to policy enhanced file based stored. Moreover, feature

sets can vary significantly, hence so do storage semantics. However, application level dependence on specific policy features (e.g. access controls) may limit customer's choice of IaaS provider.

However, since the focus of this thesis is on mitigating potential risks of vendor lock-in at SaaS layer of the cloud computing stack. Therefore, the following sub-section(s) presented below; 1) narrows the discussion parameters for SaaS application migration scenarios, and 2) serves the purpose of highlighting some but certainly not all the cases where interoperability, portability, and security are important issues when migrating in the cloud computing environment

3.3.1 Cloud SaaS Lock-in Challenges

Despite the numerous advantages of cloud computing to organisations, many challenges such as data lock-in, application lock-in and contract lock-in remain inadequately addressed. In this section, we aim to address these issues of concern as it pertains to SaaS usage and their implications to enterprise cloud adopters. We tackle the vendor lock-in challenges that act as barriers to either adopting cloud-based SaaS services in enterprises, or migrating/switching between SaaS vendors. Thus, our line of reasoning here provides a concise yet relevant discussion and in-depth analysis of these issues with some fundamental guidelines that should be observed by organisations, entering a cloud computing service SaaS contract. While it is important to understand that the extent and nature of vendor lock-in varies per the cloud type, be aware, however, that our focus within this paper is aimed at SaaS lock-in, specifically. Both PaaS lock-in and IaaS lock-in is outside the scope of this thesis.

As cloud computing adoption rate soars across enterprises (small or large), the risks of vendor lock-in is prevalent. Limited studies exist, except for (Opara-Martins et al. 2016), to analyse and highlight the complexity of vendor lock-in problem in the cloud environment. Therefore, when selecting SaaS offerings from cloud vendors, organisations need to consider and balance service criticality against the significance of avoiding potential risks of vendor lock-in. Though it is claimed that vendor lock-in is not exclusively a computing problem, since it also occurs in the classic IT setting – in which case the customer has more control over the data and services. However, (Conway and Curry, 2013) argues that due to the immaturity of current cloud computing environment, data, applications and services are primarily vulnerable to the risk of lock-in. In general, with cloud computing architectures, the risk of vendor lock-in rises with the number of hardware and software components the vendor provides. Thus, the highest lock-in risks occur with SaaS services because the vendor controls all key components of the customer's information system. SaaS lock-in affects both data and application. Besides, cloud SaaS offerings are often based on proprietary non-standard data formats and application logic, which can make migrating data and services to another cloud SaaS

vendor difficult. This potential dependency for service provision on a cloud SaaS vendor may lead to specific data and application lock-in challenges as described below.

- **Data Lock-in Challenge**: In using cloud SaaS offerings, enterprise data are typically stored in a custom database schema designed by the SaaS vendor. SaaS cloud vendors generally do not provide conceptual or logical data models for their service. Most SaaS vendors offer API calls to read and export data records. However, if the provider does not offer readymade data 'export' functionality, the enterprise will need to develop a program to extract their data and write it to file ready for import to another vendor. It should be noted that database schemas, data formats and application programming interfaces (APIs) are valuable in providing the function of interoperability of communication and processing within the SaaS cloud (Opara-Martins et al. 2014). However, the closed proprietarily coding of these key components across SaaS vendor offerings results in the need for resource (i.e. human effort, time and cost) to be focused into developing a solution to break free from having the enterprise data locked into SaaS offerings (e.g. data models, platforms and programming languages). While custom code may be needed for data transformation, it is also wise to check that standard data formats used by the enterprise can be supported by other cloud SaaS vendors or there is a transformation mechanism available. This further drives the requirement for consumers using the SaaS services to understand the business and associated data that needs to be managed to support the business process being automated or replaced, before making important migration decisions.

- **Application Lock-in Challenge**: Replacing an on-premise ICT system with its cloud SaaS counterpart benefits from the advantages of converting capital expenditure to operational cost (Sahandi et al. 2013). However, cloud SaaS applications are developed to run on a particular operating system. SaaS vendors typically develop these custom applications tailored to the needs of their target market. Porting them to operate on another cloud SaaS provider's environment is a significant effort, because the application processing logic is supplied by the vendor and data may be proprietary (Opara-Martins et al. 2016). Likewise, a company can spend a considerable amount of time and effort moving its SaaS applications (and data stored in one system) to a cloud SaaS environment due to application lock-in risks. For instance, enterprise SaaS customers with a large user-base can incur very high switching costs when migrating to another SaaS vendor as the end-user experience is impacted (e.g. re-training staffs). However, it may be easy in the case of SaaS to terminate a service from one cloud vendor and start service with another. If the terminated vendor is contractually required to provide data, migrating may be of questionable use without significant cooperation and resources provided by the vendor. For example, if the data is maintained in a proprietary

database architecture (e.g. NoSQL data models), a conversion effort will be required, and, unless the appropriate cooperation is obtained, the project may prove costlier and take longer than forecast. Furthermore, where the customer has developed programs to interact with the vendor's API directly (e.g. for integration with other applications) this will also need to be re-written to consider the new vendor's APIs. Accordingly, as pointed out by (Polikiatis, 2015), standardising on cloud SaaS environment is a serious decision with long-term financial implications for an enterprise.

The vendor lock-in challenges discussed in this section are high category risks that organisations must tackle when considering cloud SaaS solutions. They present two potential drawbacks for cloud service consumers; first, the provider has the customer organisation at a disadvantage, as it can push disagreeable terms on the customer because it has no viable exit strategy. Secondly, if the provider goes out business in the worst case, the customer may have trouble sourcing an alternative. This can take considerable time, cost and effort to find a SaaS replacement and move the entire organisation's data. However, regarding these challenges, an exit strategy will either mitigate or exacerbate the impact of such risks. There is a need for these organisations to understand what the exit strategy looks like, even if it is unlikely that they will exit a service soon – besides, no company would want to buy into a service where they feel they had no alternative provider (Opara-Martins et al. 2016). An exit strategy in this context refers to a way of moving to another SaaS vendor if the enterprise wishes to do so. Hence, a missing exit strategy is said to exacerbate data and application lock-in risks in SaaS offerings. We further elaborate on this matter in Section 3.4.5 (*sub-section C*)**.**

3.3.2 SaaS Lock-in Dimensions and Approaches for Adoption

In any relationship between a cloud SaaS service vendor and cloud SaaS consumer, vulnerabilities exist that can result in vendor lock-in situations (Burns, 2012). For example, a lack of standard technologies and unification of interfaces within the cloud stack creates barriers for migration. In today's cloud computing marketplace data, application, and services are vulnerable to the risk of lock-in. It is the cloud service customer's data that is the primary asset at risk from lock-in situations here. Hence, if a cloud SaaS customer's data cannot be migrated, accessed or retrieved due to related challenges with portability and interoperability issues at the individual levels of the cloud computing stack, business continuity is at risk. These issues consequently translate into two core dimensions of SaaS lock-in as precisely described below.

1) **Horizontal SaaS Lock-in:** Cloud service consumers face horizontal lock-in situations when vendors restrict them to freely replace a SaaS solution with a similar or competitive product offering. This situation can arise when a customer wishes to move to another SaaS solution

but is hindered by obstacles or migration limitations put in place by their vendor. This consequently affects data portability, re-creation of cloud-based services to on-premise (i.e. roll-back), integration and interoperability etc. Some of the likelihood of issues with SaaS cloud vendors or technology products which give rise to horizontal lock-in situations are; discontinuing software products without clear roadmaps for replacement, developing economically unsupportable solutions, releasing products without appropriate quality checks, vendor application highly customised to suit enterprise etc.

2) **Vertical SaaS Lock-in:** In this situation, cloud SaaS customers are restricted to the use of specific software and hardware within the overall cloud service stack because of a chosen SaaS solution. This implies also that the use of an operating system, database hardware vendor and even any required implementation (or integration) partner during migration may be dictated by vendor. At the SaaS layer, vertical lock-in can be difficult to avoid since the choice and location of hardware at the cloud provider's data centre is out of the cloud service customer's control. Thus, the idea will be to ensure whether the data centres are locked or not into a particular operating system environment through their choice of virtualization. Common issues and challenges fraught with vertical SaaS lock-in includes but not limited to enterprise infrastructure built around vendor proprietary standards, SaaS applications built using vendor proprietary APIs, data in SaaS cloud products resides in proprietary database with no ability to export, and the vendor owns data rights necessary to operate SaaS solution etc.

Therefore, while the business value of cloud computing is compelling, it is clear from raised above that many organisations still face the challenge of lock-in when adopting cloud SaaS service capabilities. With regards to cloud adoption approaches in enterprises, for simplicity, in this section, we categorise cloud computing SaaS services into two broad titles, namely: 1) horizontal SaaS offerings and; 2) vertical (or sector-specific) SaaS offerings. Horizontal SaaS offerings are typically applicable to organisations across a range of business sectors, i.e. they are not specific to a business but can be found in almost any kind of organisation. Some common horizontal SaaS applications are in the areas of email, customer relationship management (CRM), productivity, collaboration, analytics, etc. With the proven success and maturing of horizontal SaaS offerings, sector-specific SaaS offerings are emerging to include application in the areas of logistics and supply chain management (SCM), for example. Vertical SaaS offerings refer to specialised applications that will be used to support a focused business function or core processes that is found within that industry e.g. patient record management for hospitals, hotel management software etc.

The approach for adopting SaaS offerings will differ based on the IT maturity of the organisation. To help companies assess where SaaS is a strong fit, identify readiness to adopt SaaS for

a specific purchase, and address hurdles to SaaS success, we incorporated the SaaS capability maturity assessment proposed in (Herbert, 2013) into this PhD study. In corroboration with (Herbert, 2013), it is recommended that before purchasing/adopting a cloud SaaS solution, organisations should determine whether: 1) the solution category is a good candidate for software-as-a-service replacement; 2) the SaaS solution has the requisite technical capabilities to support the business requirement; 3) the organisation has development skills suitable for SaaS; 4) the organisation has an appropriate solution governance process to capitalise on the benefits of SaaS; and 5) the SaaS purchasing processes are sound. In addition, customers can negotiate contract terms to reduce SaaS lock-in risks by including the right to export data from the system in standardised formats and long-term pricing and support agreements. Being that cloud SaaS solutions are strategically engineered to have control points, making it difficult for customers to migrate away from their technology to competing solutions. Thus, it is important that customers review the SaaS lock-in discussed above, to determine cloud vendors and technologies that have the highest replacement or switching costs, and are most likely to create operational, financial or legal issues. Organisations should also analyse SaaS offerings (i.e. vertical or horizontal) in terms of Total Cost of Ownership (TCO)/Return of Investment (ROI) against associated risks such as vendor lock-in, interoperability, portability, and security, including defining a clear strategy for both private and public implementations before adopting specific SaaS offerings. Therefore, the success of cloud SaaS adoption is as much dependent on the maturity of organisational and cultural (including legislative) processes as the technology, per se. The next section presents brief analyses of some core lock-in challenges with switching cloud SaaS vendors.

3.3.3 Challenges with Switching between Cloud SaaS Vendors/Solutions

Within this work, we have initially targeted the switching difficulties and lock-in challenges of migrating between cloud SaaS vendors (whether public, private or hybrid ones). Before we delve into the core challenges to switching between cloud SaaS vendors, or retrieving the enterprise data in case of service provider failure, it is important to understand that if corporate data (or application components) is not locked-in to a specific provider moving to another cloud SaaS vendor will just be a matter of enduring a switching cost (Opara-Martins et al. 2016). Such cost can be reduced by employing best practices such as choosing cloud providers that support: (i) the use of standardised APIs wherever possible; (ii) a wide range of programming languages, application runtimes and middleware; (iii) use of simple methods to archive and deploy libraries of virtual machine images and preconfigured appliances. The option of switching and/or changing cloud service providers is a key right for cloud service consumers and enterprises. Having said that, switching cloud SaaS vendors implies that it should be possible to transfer personal and other business data to a new cloud SaaS provider in a format that is commonly useful, and without hindrance from the former provider.

However, in (Khajeh-Hosseini et al. 2012) it is argued that the complexity and cost of switching (or porting) a cloud service to a different vendor is often under-appreciated until implementation. In this aspect, functional misalignment with business needs and technical limitations in areas including integration, security, or extensibility are major inhibitors to switching from one cloud vendor SaaS service to another.

The reasons for changing from one cloud SaaS service and/or vendors to another may vary. In some cases, the SaaS service in question may be terminated by the provider due to lack of commercial success, vendor goes bankrupt, or a change in focus of business activities. While the reasons for changing SaaS vendors can provide many benefits, from the enterprise and consumer's perspectives, however being able to work with other cloud SaaS vendors without major changes is one of the main benefits of openness and standardisation. Unfortunately, many enterprise decision makers are in no position to realise this valuable opportunity to save cost by retaining the flexibility to change cloud providers to suit the organisational needs. Instead, they are burdened by the oversized, complex migration and costly integration and porting effort to handle. Thus, the gap between what the business needs and expects (in terms of switching), and what its IT group can deliver, continues to grow wider. To bridge this gap, we identify the need to examine various barriers that enterprises and cloud consumers may encounter when switching between cloud services and/or vendors in the SaaS marketplace. Our research draws on enterprise SaaS use case scenarios. Four specific scenarios have been identified in (Ahronovitz et al. 2010), and extrapolated in this paper, to depict the typical enterprise use case of working with different SaaS vendors, either adding an additional vendor or replacing an existing one. The use case purpose in our argument here is to clearly identify and discuss core system-wide issues of vendor lock-in acting as switching difficulties or barriers in enterprise SaaS migration

Based on the review of existing literature studies and the results extrapolated from our systematic study (in ***Appendix 1***), the following constraints and challenges have been identified with switching between cloud SaaS vendors: switching cost, data portability, API propagation and integration issues, interoperability and standards, security risks, contract and SLA management, and legal challenges (data location constraints, data ownership rights, cloud in/exit issues, legal jurisdiction and compliance etc.). They have been further grouped into three main challenge (i.e. technical, business environment, and legal) areas of SaaS migration, and briefly analysed below. The first four are technical constraints to the growth (i.e. in terms of migration to, and adoption) of cloud computing SaaS services, the next four are internal business environment obstacles to switching between cloud vendors once the SaaS solution has been and/or replaced, and the last four challenges are policy and legal issues intrinsic to cloud SaaS migration process. These challenges represent shared concerns that need to be addressed prior to SaaS adoption, or switching between cloud SaaS

service and vendors. They have been listed out and presented in a tabular form (refer to **Table 3.1**) along with the classification description, study reference number and citation impact to show the representativeness of each category in the total amount of references identified in ***Appendix 1***. In doing so, we employed a quantitative approach to identify the number of references dealing with each challenge area of SaaS lock-in, to raise awareness of the core cloud migration risk factors which have received more attention and support in the research community and those of which have not been so extensively analysed.

Table 3.1 Categorisation of Cloud Lock-in Challenges impeding SaaS Migration

Migration Challenges	Description	Study ID [Sn]
A) Technical Challenges	Integration issues	[S7, S11, S40, S47, S9, S12, S14, S16, S25, S32, S47, S52, S55, S56]
	API propagation	[S7, S12, S14, S16, S32, S55]
	Technical incompatibilities	[S2, S3, S4, S16, S31, S37, S45, S46, S47, S51, S55]
	Data and application compatibility issues	[S3, S4, S9, S11, S16, S18, S29, S31, S32, S34, S37, S47, S52, S54, S55]
B) Business Environment Challenges	Interoperability and standards	[S5, S7, S11, S16, S32, S35, S45, S53, S54, S55]
	Data portability issues	[S5, S7, S11, S16, S18, S32, S35, S37, S45, S53, S54, S55]
	Security risks	[S7, S10, S11, S43, S42, S51, S56, S63]
	Switching costs	[S26, S32, S37, S47, S52]
C) Legal Challenges	Exit strategy	[S15, S32, S25, S47, S52]
	Contract and SLA management	[S15, S17, S52, S56]
	Data preservation and governance issues	[S10, S41, S47, S52, S63]
	Legal jurisdiction and compliance risks	[S15, S40, S42, S51, S52, S56]

As an example, integration and data portability for instance are two core lock-in risk factors mentioned and discussed in several of the referenced studies, also indicated in **Table 3.1**. This is because as new cloud SaaS services are deployed within an existing enterprise environment the need to integrate them with various on-premise systems and other cloud services becomes important. Thus, integration task and the need to ensure data portability has increased the complexity of decision-making in respect of enterprise cloud SaaS migration (Opara-Martins et al. 2015; Adel et al. 2014; Dillion et al. 2010; Gao et al. 2011; Cusumano 2010). Therefore, as organization's struggle with the complexities of integrating cloud services with other critical systems residing on-premise, the ability to share data (i.e. portability) across these hybrid environments remains critical, and continues as more enterprise workloads and projects are committed to cloud computing SaaS services.

A. **Technical Challenges**: With the growing availability of many new SaaS offerings, companies desire common integration methods and services to support agility and the rapid proliferation of new capabilities. In this aspect, we describe related challenges of lock-in that affects core elements necessary for the smooth implementation, configuration, operation, and migration of a cloud SaaS service for enterprise adoption. Particularly, we report on how different API categories and interface types (i.e. whether standard or proprietary) can either trigger or reduce lock-in risks by offering seamless integration and compatibility within and between multiple cloud SaaS vendors, and with the enterprises internal system. The issues raised under the heading of technical challenges are:

- *Integration Problems* – as new cloud SaaS services are deployed within an enterprise the need to integrate them with various on-premise systems and other cloud services becomes important. Integration between cloud SaaS applications and on-premise systems is typically classified into three types, namely; process (or control) integration, data integration and presentation integration. The purpose of these integrations may be to perform end-to-end workflow that crosses the boundaries between multiple business capabilities or systems. Integration among cloud-based SaaS components and systems in the enterprise can be complicated by issues such as multi-tenancy, federation (i.e. combining data or identities across multiple systems) and government regulations (i.e. controls and processes to ensure policies are enforced). Moreover, enterprises should assess how other in-house capabilities such as people, processes and technology will be leveraged and integrated in their cloud SaaS strategy. Thus, integration task has increased the complexity of decision-making in respect of enterprise cloud SaaS migration (Alkhalil et al. 2014). While a new generation of cloud-based integration tools has made this process less complex and expensive, contending with the explosive growth in APIs for SaaS applications exponentially compounds the integration challenge (Opara-Martins et al. 2015). Therefore, as organization's struggle with the complexities of integrating cloud services with other critical systems residing on-premise, the ability to share data across these hybrid environments remains critical, and continues as more workloads and projects are committed to cloud services. For further discussions on integration challenges of SaaS lock-in, please refer to *Section 4.5.8.*

- *API Propagation* – each cloud vendor that provides a cloud SaaS solutions creates its own application programming interfaces (APIs) to the application. These solutions face and mix different problems (from authentication mechanisms to resource management) reflecting different interpretation (Petcu et al. 2011). This will complicate integration efforts for companies of all sizes (small or large) and locations as they struggle to understand and then manage these unique application interfaces in an interoperable way. Unfortunately, cloud

service consumers and the SaaS applications is vendor locked-in due to known portability problems. Being that every new and emerging cloud service provider have their own way on how a user or cloud application interacts with their cloud leads to cloud API propagation problem (Parameswaran and Chaddha, 2009). This kills the cloud computing marketplace by limiting cloud consumer choice because of vendor lock-in, which creates the inability to use the cloud services provided by multiple vendors including the inability to use an organization's own existing data centre resources seamlessly. Therefore, in the absence of widely accepted standards for cloud APIs and data models, organisations willing to outsource and combine range of services from different providers and on-premise systems (Hybrid IT) to achieve maximum operational efficiency will experience technical difficulties when trying to get their in-house systems to interact with cloud SaaS services. Likewise, the lack of standard APIs for cloud SaaS services brings disadvantages when migration, integration, or exchange of resources is required (Opara-Martins et al. 2014). To avoid rewriting the entire application, the cloud services hosting the components must share a compatible API.

- *Data Storage and Middleware Incompatibilities* – arises when a cloud service customer changes SaaS solution and/or middleware vendors. Whether the SaaS vendors provide similar application or middleware, the migration of documents and data from one vendor's SaaS application to another requires both SaaS applications to support common API formats for most operations supported by today's cloud services. However, in the current SaaS marketplace, cloud-based SaaS services are offered as vendor-specific solutions using different technologies and supporting technologies (Miranda et al. 2013). This heterogeneity creates incompatibilities which hinders interoperability and data portability of SaaS applications across different SaaS cloud storage and middleware vendor environments. Moreover, processing conflicts (i.e. vendor, platform or application differences) causing disruption of service may expose incompatibilities that cause applications to malfunction if a new cloud SaaS vendor or solution is chosen. This is an issue that primarily concerns data exchange, which includes metadata, and interface compatibility. While data may need to be accessible from mobile, to desktop, to mainframe, it is wise to ensure the storage format selected interoperates regardless of the underlying platform. Data storage requirements vary for different types of data. Structured data most often requires a database system, or application specific formats, whereas unstructured data typically follow any of several common application formats used by word processors, spreadsheets etc. Thus, it is important to check for compatible systems and assess conversion requirements as needed –an example being– stored unstructured data in an established portable format for both reduced storage and transfer requirements. Furthermore, minimising this incompatibility challenge is consistent

with ensuring that existing data, queries, applications and documents should be exportable from one cloud SaaS vendor solution and importable by the other.

- *Data and Application Compatibility* – moving to a SaaS cloud or switching to a new SaaS vendor/service within the cloud can be impacted by the differences in data and application architectures. Leading SaaS providers such as Saleforce.com, Amazon Web Services, and Google Apps, all provide some degree of support for moving applications and data into their environments. However, each is architected differently enough so that moving from one to another is not easy or straightforward. Hence, appropriate interoperability and portability assessments must be made to plan for adjustments required to ensure both data and application compatibility are maintained. In this direction, the use of open and published API's will ensure the broadest support for cloud interconnectability between SaaS components facilitating migrating application and data, should a change in the service provider become necessary.

B. **Business Environment Challenges**: The issues described herein are necessary to trigger a SaaS lock-in in the business context. They are discussed to encourage consistent mechanisms to enable cloud consumers and enterprises to quickly and efficiently consume SaaS by standardising interactions between cloud customers and cloud vendors. These include specifications and agreements on data and metadata formats, or on standards for interoperability, portability and security. In other words, the challenges in this category are necessary elements for the support of cloud computing activities within already existing enterprise IT infrastructures for which technology neutrality is a necessity.

- *Interoperability and Standards* – Interoperability is the ability of different cloud systems to seamlessly communicate with each other. Cloud SaaS service consumers favour interoperability as it allows them to customise their own solutions by purchasing best-of-breed services from multiple cloud vendors and to move easily between providers (Sahandi et al. 2012). With the primary benefit of cloud computing freeing up an organisation from proprietary infrastructure, it follows that open standards are desired for interoperability. Openness provides the confidence to the consumers with their business continuity planning in the event they want to switch providers. However, cloud providers and industry stakeholders are concerned, that a premature focus on standardisation to promote interoperability could hold back innovation and the evolution of better solutions.

- *Data Portability Issues* – is concerned with how enterprises can move data (or even complete application stacks) easily among cloud SaaS vendors (Opara-Martins et al. 2016). Friedman and West (2010) classify portability as a business challenge and recommend three issues to be

resolved: (i) Transparency; (ii) Competition and (iii) Legal Clarification. As more organisations use SaaS services to store and process data, the more the need for data portability has also evolved into an important component of cloud service. The question of data portability as per SaaS lock-in arises when consumers express fear of being locked-in to a single cloud SaaS vendor if the service perhaps turns out to be inefficient, time consuming, expensive or impossible to transfer data to a different cloud, or back to their premises (Opara-Martins et al, 2014). The most important data portability aspect in this case relates to the ability of the customer to switch providers and have their data transferred to the new provider quickly. Thus, the importance of data portability aids not only customer but increases competitiveness. However, as with interoperability, cloud providers and industry stakeholders are concerned that an excessive focus on ensuring data portability will limit their incentive to innovate by making it harder for them to differentiate themselves through different architectures and offerings. Concerns about meta-data also complicate efforts to ensure data portability. That is, lack of interoperable and portable formats may lead to unplanned data changes to move to a new SaaS vendor.

- *Security Risks* – different security policy or control, key management or data protection between cloud SaaS vendors may open undiscovered security gaps when moving to a new vendor or service. End to end security remains a requirement for cloud systems to ensure compliance and data confidentiality (Sahandi et al. 2012). Besides, pushing data outside the organisations boundaries means encryption is mandatory and traditional parameterised security measures are insufficient in the cloud. To ensure portability and interoperability of data in transit to, and stored within the SaaS cloud bring a need for even greater precautions than are required for traditional processing models. Not all information used within a cloud system may qualify as confidential or fall under regulations requiring protection. Hence, cloud SaaS consumers must assess and classify data placed into the cloud, and ensure security service of the SaaS vendor adhere to the same regulatory mandates organisation's data must conform.

- *Switching Costs* – are important in conventional wisdom. Switching in the cloud SaaS marketplace is not free due to the binding business relationship between a SaaS client and its vendor. Some researchers have argued that the possibility of switching makes a product less attractive and reduces a consumer's ex ante willingness-to-pay [45–46]. Whereas others have disagreed, they argue that switching costs reduce market competitiveness, raise prices, and support customer lock-in (Cabral, 2012; Farrell and Klemperer, 2007; Beggs and Klemperer, 1992; Farrell and Shapiro, 1988; Klemperer, 1987; Klemperer, 1989). For instance, Dube et al., (2009) and Shin and Suhir (2008) have demonstrated that prices may fall with low

switching costs and rise as switching costs become high. Nonetheless, switching costs affects cloud SaaS customers who encounter lock-in risks as their data are stored, managed, and maintained in a central location and proprietary database run by the vendor. For instance, once a SaaS customer wishes to stop or discontinue the use of the existing vendor/service, it must bear the costs of recovering and moving out, which is significant in most business settings. Thus, in SaaS setting, the presence of switching costs is likely to enable the vendor to charge higher prices, exploit its clients more and achieve a higher profit – in the short run at least (Ma and Kauffman, 2014).

C. **Legal Challenges**: The categorisation of legal issues include related challenges with contract, software licenses, exit process or termination of the SaaS in question, judicial requirements and law. The following legal challenges of lock-in described below are crucial constraints worth considering for enterprises with strict governance policies and regulatory (compliance) obligations, as they move data and application services across cloud SaaS environments. They include:

- *Exit Strategy* – as an organization's operational dependence on the cloud increases, so does the importance of a formal exit strategy as part of overall cloud risk management plans. Consumers' ability to have data returned upon contract termination is another issue here. Exit strategy and end-of-contract transition are major concerns amongst enterprise cloud service consumers. In terms of exit strategy, enterprises may not wish to be tied down for too long an initial SaaS contract term – hence, a long initial term may be one aspect of lock-in. Therefore, exit planning should begin as part of the cloud service/vendor evaluation and adoption planning process. Gartner recommends enterprises to have a comprehensive cloud strategy, including purposefully devised exit plans, before the first application or byte of data is hosted in the public cloud environment (Gartner Research, 2013). The cloud vendor contract should be explicit about the organisation's ownership of and right to its data and a schedule for returning those data at contract termination. Furthermore, the contract should detail the format of the data and the mechanism for moving it, and it should accommodate regular testing of the process. Therefore, it is wise to have an exit strategy in place when negotiating with a new SaaS vendor, or re-negotiating with an existing one, prior to signing the cloud SaaS service agreement (Opara-Martins et al. 2016). Insisting on requirements for supplier choice and bulk data transfer will help enterprises achieve this exit.

- *Contract and SLA Management Issues* – changing cloud SaaS vendors and/or services is in virtually all cases a negative business transaction for at least one party involved, which can cause an unexpected negative reaction from the incumbent cloud SaaS vendor. This

must be planned for in the contractual and SLA management process as part of the business continuity program and as a part of the overall governance model. If possible, perform regular data extractions and backups to a format that is usable without the SaaS vendor, and ensure the possibility of migration of backups and other copies of logs, access records, any other pertinent information which may be required for legal and compliance reasons. Expectations for meeting service level agreements (SLA's) will introduce both distance and boundary transitions that can impact abilities to meet the SLA's an enterprise must meet for their own customers or end-users (Opara-Martins et al. 2015b). Therefore, SaaS consumers must check that the SLA's from a cloud SaaS vendor is sufficient to meet the SLA's requirements for their customers. Cloud SaaS consumers and enterprises should also understand the size of data sets hosted at a SaaS solution, since the sheer price of data may cause an interruption of service during transition, or a longer transition period than anticipated.

- *Data Protection and Preservation* – cloud SaaS consumers say concerns over data protection, confidentiality, and data preservation restrict their flexibility and willingness to switch cloud services and vendors. Some organisations are concerned that certain types of legal protection associated with data entrusted with the cloud SaaS vendor will be compromised if data is moved through the cloud to other jurisdictions. Clarity about data ownership and metadata ownership is often raised as a concern. Consumers worried about data protection and preservation will ultimately have to rely on market mechanisms to assess the trustworthiness of providers in the cloud. Nonetheless, there is no guarantee that adequate market mechanisms will emerge in a timely fashion. When enterprises move corporate data to the SaaS cloud, it is not always clear what rights the cloud SaaS service vendor gains to access, modify or distribute the data (De Filippi and McCarthy, 2012). Cloud SaaS customers must understand whether data and metadata can be preserved and migrated. While cloud consumers and enterprises lack a consensus on how to address the issues surrounding data protection, preservation and ownership, industry stakeholders express concern that over-regulation of data ownership at this point within the SaaS domain in the cloud's evolution could prevent vendors from meeting user needs and improving services.

- *Legal Jurisdiction and Compliance Risks* – an enterprise using cloud based IT services is likely to have processing performed in, and data moved between, different jurisdictions. Thus, this may place constraints on the processing that can be performed, on the movement of data, and on the degree of control that the organization has. Furthermore, it is observed that existing laws and governance are insufficient to keep pace with cloud

computing service development (Opara-Martins et al. 2015b). Thus, the potential for legal disputes is considerable. In addition, legislative and jurisdictional challenges may also arise due to the possibility of data centres located in areas with different jurisdiction. Bear in mind that many jurisdictions will have specific requirements and regulations regarding the location of data. Therefore, such requirements should be carefully considered by enterprises before a decision on adopting the cloud service model is made.

3.3.4 Standards-based Cloud Computing Services and Tools: Interoperable and Portable Cloud Standards

Interoperability and portability are central to avoiding lock-in, whether at the technical, service delivery or business level, thus ensuring broader choice and a level playing field. Open standard interfaces protect users from vendor lock-in, helping to avoid significant migration costs whenever open interfaces are not provided. The implementation of a core set of internationally recognised standards is key to avoiding multiple, inconsistent guidelines and bespoke solutions. According to a report by published by the Cloud Council (2011), standards-based cloud computing ensures that clouds can readily interoperate based on open standard interfaces. This allows workloads to be readily moved from one cloud to cloud and services created for one cloud computing environment to be employed in another cloud computing environment, eliminating the need to write redundant code. In the absence of open standards, enterprises are forced to select proprietary environments that lead to vendor lock-in. This means that integrating applications or services across differing proprietary cloud platforms will be possible but will require extensive, expensive, and time consuming work.

To avoid vendor lock-in and facilitate information sharing between different services, it is mandatory for different clouds to share and access information located in different cloud providers by using open-source APIs, for example. Such open-source approach will allow its API use by the developer community, and promote it in an effort to create a reference framework that will contribute to the development of cloud applications, eliminating vendor lock-in at and performing application monitoring at the various SPI (SaaS, PaaS and IaaS) level. Using the taxonomy developed by the NIST Cloud Computing Reference Architecture and Taxonomy Working Group, cloud computing relevant standards have been mapped to the requirements of portability, interoperability, and security. Present areas with standardization gaps include: SaaS functional interfaces; SaaS self-service management interfaces; PaaS functional interfaces; business support / provisioning / configuration; and security and privacy. Present standardization areas of priority to the federal government include: security auditing and compliance; identity and access management; SaaS application specific data and metadata; and resource description and discovery.

3.3.5 Benefits of Standardisation in the Delivery of Enterprise Cloud-based Services

Cloud providers use different types of service delivery models to provide IT services to consumers. Understanding the relationship and dependencies between the service models is critical to understanding the risks of vendor lock-in. Some service models stand to benefit from standardization than others. Enterprises moving to the cloud typically have three service delivery options (as described earlier in *Section 2.4.1*).

a. *Software as a Service (SaaS):* Benefits of standardization for SaaS are limited. For SaaS offerings, taking Salesforce.com CRM for instance, the user is an end user. Although other SaaS offerings exist in which the user can be the developer (Google Maps for example), who is responsible for integrating functionality from these services into other applications (Google, 2012). In the latter case, standardized APIs are useful because they facilitate the development process (Linthicum, 2010). However, unless the APIs are identical from a functional view, this standardization helps little with migration. Migration for the case when SaaS user is an end user would occur in the same way as with any software migration because each SaaS provider will have its own processing logic (i.e. different ways to license software) (Harding, 2010). In this case, SaaS will only benefit from standardization around data storage because the most prominent concern for SaaS consumers, especially for enterprise SaaS such as CRM, is how to extract their data (Lewis, 2012). To further substantiate using the following scenario whereby an online cloud storage service provider goes out of business for instance, in effect customer's access to their data is shut down. In this case, the consumer would have to extract its data from the cloud storage provider, write business logic to perform data transformations, and then upload data to a new service provider. The standardized APIs could potentially make this task easier.

b. *Platform as a Service (PaaS):* PaaS model benefits more from standardization than SaaS. Enterprise organizations that buy into PaaS offerings are allured by the perceived advantages of the development platform. The platform provides many capabilities out of the box, including but not limited to the following: managed application environments, user authentication, data storage, reliable messaging and other functionalities in the form of libraries that can be integrated into applications. Buying into PaaS provider means buying into a platform (with functionality tied to a specific language and runtime environment) in the same way that organizations traditionally have, which is based on added value, skills, cost and any other criteria. However, consumers can reap the incentives for PaaS adoption by selecting platforms that support more standardized tools and languages, thereby making enterprise application and data more interoperable and portable.

c. *Infrastructure as a Service (IaaS):* According to (Badger, 2012), IaaS is the service model that would benefit the most from standardization because the building blocks of IaaS are workloads represented as VM images and storage units that vary from typed data to raw data. For example,

in terms of workload migration in IaaS model, standards efforts from OVF and Virtual Hard Disk (VHD) would allow users to extract an image from one provider and upload it to another provider. For enterprise data migration in IaaS, standards initiatives like Cloud Data Management Interface (CDMI) and the Amazon Simple Storage Service (S3) API, which multiple providers support, would enable users to extract data from one cloud provider and upload it to a different provider. These standards, however, are more useful for raw data that is not typed (e.g. VM images, files, blobs) because the cloud resource in this case acts as a container and usually does not require data transformation. For typed data, enterprise data migration would occur similarly to any other data migration task: users must extract data from its original source, transform it to a format compatible with the target source, and upload it into the target source which could be a complex process as noted by (Fogarty, 2011). In addition, the effort required for data transformation will also depend on factors such as similarity between targets and source's data-storage technologies and the similarity of the interface operation.

Therefore, to understand which part of the spectrum of cloud systems is most appropriate for a given need, an organization should consider how clouds can be deployed (i.e. cloud types), what kinds of services can be provided to customers (i.e. service models), the economic opportunities and risks of using cloud services (economic considerations), the technical characteristics of cloud services such as performance and reliability (operational characteristics), typical terms of service (service level agreements), and the security opportunities and risks (security). But since the focus of this writing is not exclusive to cloud deployment or service delivery models, but to evaluate the impact of vendor lock-in problem for enterprise migration. Thus, it becomes an imperative to briefly highlight the different delivery models, in context of vendor lock-in, to identify which would benefit most from standardization efforts. Further, enterprise and SME organizations should be aware that, the different deployment models for cloud computing migration present several trade-offs in how customers can control their resources (see **Figure 2.6**), and the scale, cost, and availability of resources. Furthermore, enterprises should realize also that the different service delivery models have different strengths and risks, and are suitable for different customers and business objectives.

3.4 Emerging Standards in Cloud Computing

Research has shown that whenever a new technology attracts a great deal of attention, neither vendors nor customers is likely to wait for mature standards to emerge. Instead, they leverage the advantage of early adoption of emerging technology at the price of having to move to a standard environment later (Cloud Council, 2011). Such standards are referred to as de facto standards (i.e. market-driven standard which has not been defined or endorsed by industry groups or standards organisations). However, market-driven standards can become de jure standards if they are approved through formal

standards organisations. About cloud interoperability and portability, presented below is a summary of emerging standards aimed at addressing the cloud lock-in problem.

a. **TOSCA:** Topology and Orchestration Specification for Cloud Applications (TOSCA) is an Organization for the Advancement of Structured Information Standards (OASIS) language used to describe both the topology of cloud-based Web services, consisting of their components, relationships, and the processes that manage them, and orchestration of such services, which is their complex behaviour in relation to other described services (TOSCA, 2013). The combination of topology and orchestration, accurately describes all the essential elements needed by each service to provide its functionalities, to ease deployment in different environments and to enable interoperability. Moreover, it supports also the management of services, when applications using them are ported to different cloud platforms, throughout their complete life cycle. In summary, TOSCA's purpose is to enhance portability and interoperability of cloud applications, and related IT services, by defining an interoperable description of cloud services, the relationship between components of these services, their operational behaviour, which is independent of the cloud provider offering the services and of the technologies involved. Please refer to ***Section 4.6.5.1***.

b. **CIMI:** Cloud Infrastructure Management Interface (CIMI) is standard proposed by the Distributed Management Task Force (DMTF) which specifies an interface, represented by a set of RESTful APIs, to manage cloud platforms operating at an IaaS layer (Demchenko et al. 2013). Essentially, CIMI focuses on the description of the management interface of a cloud infrastructure. However, CIMI does not extend beyond infrastructure management to the control of the applications and services that the consumer (cloud client) chooses to run on the infrastructure provided as a service by the provider. CIMI allows interoperability between a consumer and multiple providers that all offer the standard CIMI interface for managing a cloud infrastructure. The interface uses Hyper Text Transfer Protocol (HTTP) to send and receive messages that are formatted using either Java Script Object Notation (JSON) or the eXtensible Markup Language (XML) (CIMI, 2012).

c. **CDMI:** Cloud Data Management Interface (CDMI) is a standard for managing data on cloud platforms, proposed by the Storage Networking Industry Association (SNIA). CDMI defines a functional interface that users and applications can use to create, retrieve, update, and delete data elements from cloud storages (CDMI, 2012). Using the interface, clients can also discover the capabilities offered by the cloud platform and manage the containers and the data that is placed in them, together with meta-data associated to both containers and data. The CDMI standard describes cloud storages through a file system-like structure, in which data objects contain the stored data and are organised as files in a hierarchical directory, where folders are instead represented by containers (Martino et al. 2015).

d. **OCCI:** Open Cloud Computing Interface (OCCI) is a RESTful protocol and API, published by the Open Grid Forum (OGF). The objective of the proposed standard is to define a shareable and homogenous interface to support all kinds of management tasks in the cloud environment. As enterprises move into the cloud, the deployment of their data and the applications becomes very important to them. As such, there is a demand for ensuring clean interfaces and protocols which are easy to use and can be used for multiple kinds of service offerings to prevent a vendor lock-in. In the context of these developments, the OCCI working group works towards forming such a standard. The OCCI family of specifications can be used for IaaS and PaaS offerings (Edmonds et al. 2011). It strives to create an open, interoperable protocol and API for the Cloud. The OCCI protocol can be used for integration, ensuring interoperability and portability between service providers. Proprietary APIs can be used alongside OCCI in the case that other features than those of OCCI are maintained. Generally, the specification strives to be very easy, flexible and extensible.

e. **OVF:** DMTF Open Virtualization Format (OVF) standard for packaging and distributing virtual appliances enables portability and simplifies installation and deployment of virtual appliances across multiple virtualization platforms. A virtual appliance is a pre-built software solution, comprised of one or more virtual machines (VMs) that are packaged, maintained, update and managed as a unit (DMTF, 2008). By creating virtual appliances, software developers and independent software vendors (ISVs) can package and ship pre-installed, pre-configured solutions that enable end-users to literally plug into their environments with minimal effort. Customers also get greater flexibility by facilitating the mobility of virtual appliances across diverse virtualization platforms. With virtual appliances, installing, configuring, and maintaining enterprise software is simplified, resulting in a better IT administrative experience. **Figure 3.7** shows where OVF standards fit into a virtual appliance life cycle.

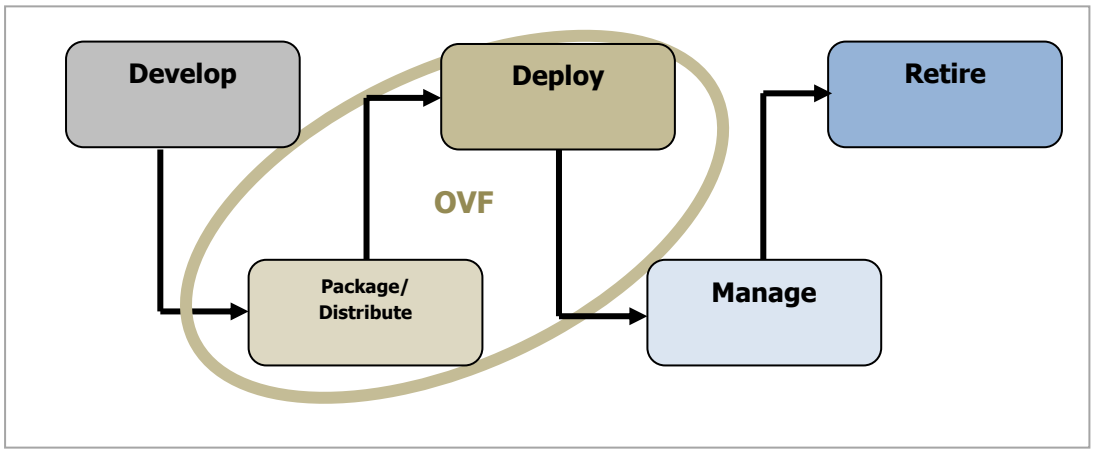


Figure 3.7- OVF Scope in Software Life Cycle (Adapted from [OVF, 2008])

3.5 Cloud Computing Security Analysis

There is so much concern about security within the cloud computing environment (Zissis and Lekkas, 2012). Cloud computing presents its own set of security issues coupled with the risk and threats inherent in traditional IT computing. But as enterprise boundaries have been extended to the cloud, traditional security mechanisms are no longer suitable for applications and data in the cloud. Security in cloud computing ranges from physical security (facilities), to network security, to the IT systems security, and all the way to the information and application security. The applications and corporate data being hosted by cloud service providers are prone to vulnerabilities from unauthorized parties (Carroll et al. 2011). In addition to the usual challenges of developing secure IT systems, cloud computing presents an added level of risk because essential services are often outsourced to a third party (IBM, 2009). The externalized aspect of outsourcing makes it harder to maintain data integrity and privacy, support data and service availability, and demonstrate compliance. In effect, cloud computing shifts much of the control over data and operations from the client organization to their cloud providers (as illustrated in **Figure 2.6**), much in the same way that organizations entrust part of their IT operations to outsourcing companies. Thus, clients (i.e. consumers and end-users) must establish trust relationships with their providers and understand risk in terms of how these providers implement, deploy and manage security on their behalf. This trust relationship between cloud service providers and clients is critical because the clients are still ultimately responsible for compliance and protection of their critical data, even if that workload has moved to the cloud.

To put security in perspective, cloud computing can be considered the ideal use case to highlight the need for a consistent, transparent, standards-based security framework regardless of cloud deployment model. As companies move or build solutions in the cloud, having this consistent security model is vital to simplify development and to avoid vendor lock-in and preserve their IT investments. The most significant difference when considering security from a cloud perspective is the enterprise's loss of control, as opposed to any technical challenge. With an in-house application, controlling access to sensitive data and applications is crucial. Whereas, with a cloud-based application, access control is just as important, but the infrastructure, platform and application of security is under the direct control of the cloud provider.

Subashini and Kavitha (2008) made an investigation of cloud computing security issues from the cloud computing service delivery models (SPI model) and give a detailed analysis and assessment method description for each security issue. Morsy et al. (2010) explored the cloud computing security issues from different perspectives, including security issues associated with cloud computing architecture, service delivery models, cloud characteristics and cloud stakeholders. Chen et al. (2010) believed that two aspects are to some degree new and essential to cloud: the complexities of multi-party trust considerations, and the ensuing need for mutual auditability. They also point out some new

opportunities in cloud computing security. According to IDC (2009), security is considered a key requirement for cloud computing consolidation as a robust and feasible multipurpose solution. This viewpoint is shared by many distinct groups, including academia researchers (Armbrust et al. 2009; Rimal et al. 2009), business decision makers (Shankland, 2009) and government organisations (Catteddu and Hogben, 2009; CSA, 2009). Due to the growing interest in cloud computing, there is an explicit and constant effort to evaluate the current trends in security for such technology (Gonzalez et al. 2012). An authoritative reference in the area is the risk assessment developed by the European Network and Information Security Agency (ENISA) (Catteddu and Hogben). This reference document, not only lists the risks and vulnerabilities, but it also offers a survey of related works and research recommendations. A similar work is the security guidance provided by the Cloud Security Alliance (CSA, 2009), which defines security domains, ranging from governance and compliance to virtualization and identify management. These issues discussed in the aforesaid works require further studies for being appropriately handled and, consequently, for enhancing technology acceptance and adoption (Gonzalez et al. 2012). Enterprises must take note of such issues when consuming cloud services. Moreover, there are other aspects about cloud computing that also require a major reassessment of security and risk. For example, inside the cloud, it is difficult to physically locate where data is stored. Security processes that were once visible are now hidden behind layers of abstraction. This lack of visibility can create many security and compliance issues. Therefore, organisations require visibility into the security posture of their cloud. Visibility can be especially critical for compliance. Thus, security is a crucial aspect for providing a reliable enterprise IT environment, and to enable the use of applications in the cloud and for moving data and business processes to virtualized infrastructures.

3.6 Cloud Service Contract Agreement

According to Leimbach et al. (2014) contractual relationship between cloud service providers and their clients is laid out in one or more documents comprising: Terms of Service (ToS), SLA, and Acceptable Use Policy (AUP). In (Hon et al. 2012), it is claimed that the starting point for cloud contracts is usually the providers' ToS – which are provider favourable (ibid). However, recent research by (Bradshaw et al. 2010) notes distinctions in terms and conditions governing cloud service contracts: free vs. paid services. Within paid services, terms and conditions typically fall into those offering standard form contracts and those subject to negotiation. Though the latter typically are limited to those perspective customers with sufficient bargaining power, but the former comes with common challenges in that, many cloud service providers reserved the rights to change contract terms unilaterally. Moreover, as highlighted above many cloud providers' term may already not be suitable to accommodate specific (especially enterprise users) requirements. Thus, some cloud consumers will seek changes to make the terms more balanced and appropriate to address own circumstances and

meet their heightened security requirements. But, as with other outsourced IT provision, a good service agreement is crucial in this case.

An SLA generally details the level of service to be provided and includes mechanisms for auditing service delivery, and a mechanism for compensating clients for underperformance. Besides, failure to meet performance level in cloud service agreements can result in significant losses and damages for a business. Thus, an SLA should reflect organisations requirements in areas such as data security, business continuity and disaster planning (JISC Legal, 2011). Unlike traditional Internet services, standard contract clauses may deserve additional review because of the nature of cloud computing. For this reason, it is recommended that businesses ensure whether and how cloud providers support data portability and interoperability – prior to signing the cloud service contract. Besides, as noted by (Hon et al, 2012), application portability is one aspect of dependence risk which is not discussed as much as data portability, whether by our sources or in the literature. However, it is equally if not more important, particularly for IaaS and PaaS. Therefore, as cloud use becomes more widespread and sophisticated, it is believed that future contract terms may extend to cover application portability, virtual machine portability, and perhaps even interoperability. In addition, there are standardization efforts that specifically address lock-in issues in the cloud as presented in *Section 2.8.3*. One possible way businesses can reduce potential lock-in effect at pre-contractual phase is to at least understand the commonalities among provider interfaces, evaluate vendors/providers for cloud specific interoperability and portability standards, before choosing cloud providers. Furthermore, organisations should also pay attention to their rights and obligations related to notifications of breaches in security, data transfers, and access to data by law enforcement entities (e.g. e-discovery).

Since the cloud can be used to outsource critical internal infrastructure, and the interruption of that infrastructure may have wide ranging effects. For these reasons, organisations should carefully consider whether standard limitations on liability adequately represent allocations of liability, given the organisations' use of the cloud, or responsibilities for infrastructure. This will require a scrutiny to the rules governing data flow within and outside the UK. In conclusion, while adopting a cloud service or provider may be easy; migrating to another is not (Claybrook, 2011). After moving local data and processes to the cloud, the lack of standards for protocols and formats directly affects attempts to migrate to a different provider even if this is motivated by legitimate reasons, for example non-fulfilment of SLAs, outages or provider bankruptcy (CSA, 2011). Consequently, the first choice must be carefully made, as SLAs are not perfect and services outages happen at the same pace that resource sharing, multi-tenancy and scalability are not fail proof (Gonzalez et al. 2012). After a decision is made, future migrations between services can be extremely onerous in terms of time and costs; most likely, this task will require an extensive work for bringing all data and resources to a local infrastructure before redeploying them into the cloud. In summary, enterprises should ensure when choosing cloud providers to select providers' whose standard contract terms encourage the

development of a full variety of cloud services and contract terms priced at different levels, with standards and certifications to assist with legal uncertainty regarding compliance.

In summary, an SLA is the foundation of the consumer's trust in the provider. A well-written SLA codifies the provider's reputation. The marketplace features two types of SLAs: Off-the-shelf agreements and negotiated agreements between a provider and consumer to meet that consumer's specific needs. It is unlikely that any consumer with critical data and applications will be able to use the first type. Therefore, the consumer's first step in approaching an SLA (and the cloud in general) is to determine how critical their data and applications are. It is crucial that the consumer of cloud services fully understand all the terms of the provider's SLA, and that the consumer consider the formal needs of their organization before signing any contractual agreement.

3.7 Survey of Existing Frameworks, Tools and Decision Support Systems for Cloud SaaS Migration

Cloud computing adoption decisions are challenging due to various concerns such as cost, confidentiality and control (Khajeh-Hosseini et al. 2012). However, migration to the cloud computing SaaS environment is a strategic organizational decision. Using a reliable framework for migration ensures enterprise stakeholders to mitigate vendor lock-in risks in the cloud SaaS solutions. Therefore, organizations always search for cloud migration frameworks with dynamic nature as well as integrity beside their simplicity (Bazi et al. 2017). In practice, migrating business systems to the cloud is associated with a change in the risk landscape to an organisation (Cayirci et al. 2016). European Network and Information Security Agency (ENISA) and Cloud Security Alliance (CSA) have found that vendor lock-in risks and insufficient due diligence were among the top threats in cloud computing (Dutta et al. 2013). Organisations that adopt, or migrate to, cloud computing services often do not understand the resulting risks. Hence, decisions to migrate existing enterprise systems to SaaS solutions can be complicated as evaluating the benefits, risks and costs of using cloud computing is not straightforward (Khajeh-Hosseini et al. 2011). Migrating to or replacing existing systems with cloud-based SaaS solutions is a multi-dimensional problem that spans beyond technical issues and into the financial, security and organisational domains (Andrikopoulos et al. 2013). Given that cloud services could be characterized using multiple criteria (cost, pricing policy, performance etc.), it is important to have a methodology for selecting cloud services based on multiple criteria (Furht, 2010). Additionally, the end user requirements might map to different criteria of the cloud services. This diversity in services and the number of available options have complicated the process of service and vendor selection for prospective cloud users and there is a need for a comprehensive methodology for cloud service selection (Rehman et al. 2011). For instance, when several vendors offer, SaaS based products, the selection of product becomes a key issue as it involves analysis of selection parameters and product offerings of the vendors. This problem needs thorough understanding of requirements and

product offerings. The selection process involves multiple criteria and multiple products; hence, selection based on judgements fails to identify suitable choice.

3.7.1 Making Informed Decision When Selecting Cloud-based SaaS Products

SaaS selection based solely on mere judgment is a highly cognitive and tedious process which could be quite error prone (Godse and Mulik, 2009). If a problem is decomposed into clusters, and attributes are compared pair wise within the cluster, then decision problems can be solved easily with reduced cognitive load. Therefore, the selection of cloud SaaS products is a multi-criteria decision-making (MCDM) problem as vendors with the best technology are not always suitable for a given enterprise (Whaizduzzaman et al. 2014). Being that MCDM problems cannot be solved with mere judgement or intuition, it is necessary therefore to have quantifiable values instead of subjective opinions to make an informed decision (Godse and Mulik, 2009). Analytic Hierarchy Process (AHP) method is very useful in simplifying such MCDM problems into hierarchy thus forming the comparison matrix to judge the weight. The AHP deals with intuitive, rational and/or irrational, multi-objective, multi-criteria decision making with certainty and/or uncertainty for any number of alternatives. It breaks down a problem into its smaller constituent parts forming hierarchy and then calls for only simple pair-wise comparison judgments. An advantage of hierarchy is that it allows focusing judgment separately on each of the several properties, which is essential for making a sound decision. Though, a good amount of cloud computing research has been reported in the areas of SaaS configurability (Nitu, 2009), security, integration (Hudi et al. 2009), networking challenges (Greschler and Mangan, 2009), and business model (Liao and Tao, 2009). However, there is no explicit guidance available on selection of interoperable and portable SaaS product for business application. To further complicate matters, Garg et al. (2013 and 2011) have also acknowledged that moving applications and/or data into the cloud is not straight forward. Numerous challenges exist to leverage the full potential that cloud computing promises. These challenges are often related to the fact that existing applications have specific requirements and characteristics, which need to be met by cloud providers. The key problem with the studies cited herein is that they focus only on migrating applications without taking into account other factors such as organisational issues of cloud vendor lock-in problem. Moreover, what becomes obvious in the preceding section(s) is that migrating to, or switching between SaaS vendors in the cloud requires making several decisions related to how the challenges of lock-in can be mitigated at pre-and post-deployment management stage(s). Organisational and socio-technical factors must also be considered during the decision-making process as the SaaS cloud migration process will result in noticeable changes to how systems are developed and supported (Khajeh-Hosseini 2010).

3.7.2 Decision Frameworks for SaaS Cloud Migration

A lack of awareness of standard methodologies or guidelines adds difficulty in the formation of an estimate for quickly and effectively migrating applications from one cloud provider platform to another. A series of works on decision frameworks for the migration of enterprise applications and data to the cloud have appeared in the current literature. An example is the Cloudward framework (Hajjat et al. 2010), was developed in collaboration between academic and industrial partners with the goal of migrating enterprise applications to hybrid cloud solutions. The framework considers cost savings, communication costs, transaction delays and constraints like security, however no explicit discussion is made about how the vendor lock-in problem can be avoided or mitigated. The Cloud Adoption Toolkit (Khajeh-Hosseini et al. 2012) is another proposal that provides a framework specifically aimed at enterprise stakeholders. For this purpose, the framework provides the means for tasks like technology suitability analysis based on the profile of the enterprise, cost modelling and energy consumption analysis for the to-be model of the migrated systems, as well as responsibility modelling distinguishing between operations, maintenance and management roles for migrated and non-migrated system components. These tasks are meant to be performed in a sequential manner, forming a decision-making process. Again, no discussion is offered in the aforesaid work on how the risks of vendor lock-in should be managed during the migration process. In a similar fashion, the CloudStep (Bassera et al. 2012) approach provides a decision process consisting of nine activities including enterprise, legacy application and cloud provider profiling, constraint identification analysis and alternative migration scenarios evaluation and ranking. Constraints that are taken into consideration are categorized in seven areas: financial, organizational, security, communication, performance, availability and suitability. Banerjee (2012) explored existing cloud migration methods and identified challenges that impede effective utilisation of cloud services. He concludes that there is no one-size-fits-all cloud, and it is up to each business to decide how much change is tolerable and to decide how far into the cloud to step. Decision making for cloud computing migration was investigated by a number of studies (Song, 2013; Alkhalil et al., 2014; Andrikopoulos et al., 2014; Rehman et al., 2015). However, these studies share a limitation in that they focus on developing decision making tools to support application migration and consider technical and cost aspects only, and they did not discuss organisational and strategic issues. Latif et al. (2014) presented a systematic review of cloud computing risks from a cloud service perspective as well as client perspective, and in the same context Hashizume et al. (2013) highlighted the main issues related to cloud security, although neither study considers all aspects of the cloud migration vendor lock-in problem discussed in *Section 3.4.5*. There has been a limited evaluation of cloud migration. Some empirical studies identified cloud adoption factors (Khajeh-Hosseini et al., 2010; Alshamaila et al., 2013; Carcary et al., 2013; Chang et al., 2013; Lian et al., 2014). There have also been a few industry and vendor studies, however these tend to be vendor specific, as with the Amazon, Cisco, and IBM migration strategy,

which is built around the Amazon Web Services (AWS) platform (Varia, 2010), Cisco cloud computing infrastructures (Cisco, 2010), and IBM systems (Banerjee, 2012) respectively or else consider only a subset of issues (Parakala & Udhas, 2011).

Chauhan and Babar (2012) present a high level seven decision step process built on best practices and lessons learned from the migration of legacy application to service-oriented architectures. Silva et al. (2013) conducted a literature study on how migration of applications to the cloud is realised and identified three classes, namely: 1) standardised format migration, 2) component format migration, and 3) holistic migration. Their conclusion is that current cloud migration research approaches do not offer a holistic view, instead focuses on the standardised format of migration to enable portability. To overcome this challenge, they proposed the Cloud Motion (CMotion) framework which leverages existing application models and provides support to migrate composite applications into and between clouds. Kaisler et al. (2012) developed a decision framework to assist IT managers who are determining which cloud solutions matches their specific requirements and evaluating the numerous claims of a cloud's value. This decision framework helps enterprise managers allocate investments and assess cloud alternatives that now compete with in-house data centres.

3.7.3 Systematic Reviews on Cloud Migration Approaches

Silva et al. (2013) conducted a systematic literature review to identify, analyse and classify existing solutions to cloud lock-in, and highlight unresolved challenges. Their survey is a based on a systematic review of 721 primary studies that describe the state-of-the-art in managing cloud vendor lock-in problem, interoperability and portability. Their review results show that most solutions proposed so far are platform-oriented, APIs, or architectures addressing infrastructure-as-a-service (IaaS) interoperability. However, most importantly their review also identified the need for addressing the socio-technical, business and legal challenges related to cloud lock-in. Andrikopoulous et al. (2013) built on existing works and solutions for the migration of enterprise systems and applications to cloud solutions, and thus proposed a decision support framework. Their framework focused on supporting decision makers in evaluating the need for migration of enterprise systems, and guiding them along the decisions that need to be made before the actual migration process. Iyer and Henderson (2010) identify seven potentials of cloud computing. The implementation of each of them needs expenses. By analysing these costs and the intended value of the migration to cloud computing, organizations can decide if it benefits them to adopt. Finally, Jamshidi et al. (2013) provide a systematic review of the state-of-the-art on methodologies, techniques, tooling support and research directions. Their conclusion is that the field is still at a formative stage, and that cross-cutting concerns like security and effort estimation are not being addressed sufficiently. Yet again, the vendor lock-in problem has not been considered as part of the cross-cutting concerns which require further

research investigations. To compare, in terms of research methodology, the work of (Silva et al. 2013) is the closest to ours (refer to ***Appendix 1***). However, we focus on the socio-technical, business, and legal challenges related to cloud SaaS lock-in. On the other hand, in terms of conceptual cloud decision frameworks to avoid the risks of vendor lock-in during service migration and integration, the work of (Bassera et al. 2012) is the closest to ours. Nonetheless, in summary, according to authors' recent work (Opara-Martins et al. 2017) and best knowledge, in conjunction with discussions of empirical findings *Section 4 and Section 5*, it is believed that the work resulting from this PhD thesis is the first attempt to consolidate cloud migration and vendor lock-in research studies together – with an emphasis on identifying all key interoperability and portability aspects for vendor-neutral SaaS application domain.

3.7.4 Concluding Remark

The difficulties faced by organisations in moving their applications and business systems to the cloud have picked interest from the research community, with several works having recently been published on this topic, e.g. (Saripalli and Pingali, 2011; Bibi et al. 2010; Zardari and Bahsoon, 2011). In recent years, several experience reports have started appearing discussing the replacement and migration of existing systems and applications to cloud solutions (Chauhan and Babar, 2011; Khajeh-Hosseini 2010), illustrating the multi-dimensionality of the problem. While some of these works are reports of case studies involving the migration of existing legacy systems to the cloud, others focus on proposing techniques and tools specifically aimed at supporting cloud adoption decisions. Still, none of these works have presented a detailed methodological framework detailed to be useful as a guide for cloud SaaS consumers and enterprises mitigating vendor lock-in risks in a typical cloud migration scenario. For example, Jamshidi et al. (2013) provide a systematic review of the state of the art on methodologies, techniques, tooling support and research directions for migrating applications to cloud solutions. The conclusion drawn from their work showed that the field of cloud migration is not yet mature but still at a formative stage, and that cross-cutting concerns like security for instance are not being addressed.

Current decision frameworks for cloud computing adoption in enterprises focus on the migration of the application (or enterprise system) to the cloud environment (Andrikopolous et al. 2013), estimation of the application load (Bankole and Ajila, 2013), or the costs when deploying the application (Sulieman et al. 2012), (Liew and Su, 2012), among others. However, their proposed solutions do not provide a structured or organised process in which the cloud SaaS consumers can methodically check their choices for potential lock-in risks when planning the deployment and executions of SaaS applications in the cloud. There is a need for a framework (with guidelines) and decision support tools for enterprises that are considering either consuming or moving their IT systems to cloud-based SaaS solutions. Cloud providers on the one hand are attempting to address this

demand with white papers offering advice (Varia 2010; Chappel, 2009), while IT consultancies on the other hand are offering frameworks (Ward et al. 2010; Computer Sciences, 2010; Accenture, 2009; Alonso et al. 2013; Tan et al. 2013; Donnellan et al. 2011; Garg et al. 2013; Chen et al. 2013) and assessment tools (Computer Sciences, 2010; Accenture, 2009; Herbert, 2013; Microsoft, n.d.), to support decision makers. Such tools are either marketing tools or they are not widely available as they are based on closed proprietary technologies that are often accompanied by expensive consultancy contracts (Khajeh-Hosseini et al. 2011). However, the work in (ibid) discusses the vision of a system that supports decision-makers in deciding whether and how to migrate their applications to cloud solutions. So far, the existing frameworks and decision support tools, mainly focuses on IaaS solutions which provide a multi-criteria approach for application migration to cloud computing solutions. However, while some of these works are built on the success of infrastructure virtualisation solutions (like Amazon Web Services and Google Apps etc.), they still do not specifically consider the risks of vendor lock-in as per how it needs to be mitigated and avoided in the cloud environment. Moreover, the steadily increasing dominance of cloud SaaS solutions in the software market means that existing enterprise systems and applications may need to migrate to this cloud computing environment. Appropriate decision support frameworks, tools and processes are therefore needed to make cloud SaaS consumers aware of the issues of cloud lock-in. But, the existing works and research efforts in the SaaS domains, e.g. (Alonso et al. 2013; Tan et al. 2013a; Tan et al. 2013b) paints a picture of immaturity too, thus requiring the introduction of a comprehensive framework with strategic guidelines to support an enterprise migrating to cloud computing services. To deliver the advantages of cloud SaaS services, and overcome the challenges of vendor lock-in faced by organisations that want to procure and migrate to cloud-based SaaS offerings, there is now a need for a decision framework on how to avoid the risks of a single provider lock-in.

3.8 Chapter Summary

This chapter provides a comprehensive analysis of cloud computing vendor lock-in problem, and proposed taxonomy of cloud lock-in perspectives. The three main perspectives of cloud vendor lock-in problem(s) are: business (or economics) perspective, technical (or technological) perspective, and legal (or political) perspective. Together they provide a complete picture of cloud computing vendor lock-in challenge. The concerns addressed in each of the perspective have been precisely and concisely discussed in this chapter. The complete organisation of the proposed taxonomy is depicted in **Figure 3.6**. The hierarchical categorisation approach used in **Figure 3.1** assists in demonstrating how each element of vendor lock-in relates to several other components in the architecture of a cloud computing system. At a high level, the model establishes a common language (i.e. ontology) for easy understanding and communication of the capabilities and requirements which should be standardised in a cloud environment to facilitate open collaboration and interoperability amongst cloud providers – thereby avoiding the risk of a single provider lock-in for cloud consumers. At a low level the model is

further composed into taxonomy to support consumers cloud service selection and adoption strategy in terms of validating cloud provider's solutions to achieve architectural integrity of business solutions of an enterprises' cloud ecosystem. In contrast to existing works, our study extends the scope of cloud computing migration beyond one specific challenge area, instead it addresses the vendor lock-in problem from three main perspectives or categories– thereby contributing substantially to the growing body of knowledge on cloud computing. Note, the associated elements of vendor lock-in used in the proposed taxonomy have been identified from authors' previous work (Opara-Martins et al. 2014, Opara-Martins et al. 2015a, Opara-Martins et al. 2015b; Opara-Martins et al. 2016) and validated with a systematic literature review (SLR) conducted (see ***Appendix 1***).

The review has identified that although there are numerous studies which consider different aspects of the cloud migration process in detail, a comprehensive, holistic framework to support decision making to avoid vendor lock-in risks for enterprise cloud migration and adoption has not been identified from the literature. As shown in the tables in ***Appendix 1***, the SLR is based on different studies which primarily focus on the technical rigor of content presented. These studies were analysed in the context of SaaS lock-in (and related migration challenges) and potential solutions by evaluating the number of citations for each referenced study including their overall research contributions. In this case, author employed a quantitative approach to identify the number of references dealing with each challenge area of SaaS lock-in, to raise awareness of the core cloud migration risk factors which have received more attention and support in the research community and those of which have not been so extensively analysed. We present the SaaS lock-in risks and related migration challenges using pie charts to show the representativeness of each category in the total amount of references identified. Through integral analysis, ***Appendix 1*** is presented to analyse current research contributions and gaps that need to be filled in terms of SaaS cloud migration problems and solutions by evaluating the number of citations for each included study.

In summary, there is no single solution to the SaaS lock-in problem in the cloud, since the choice of method for migration depends on the goals (i.e. reasons for organisations to migrate to cloud-based environments), the available budget and resources and the time needed to complete the initial migration project (Almonaies et al. 2010). Therefore, migration to SaaS cloud environment requires considering the specific migration strategy according to legacy system and existing SaaS solution. If existing SaaS solution has the same business functionality of legacy system, for example, users can replace legacy system by SaaS. Whereas, when some business functionality has been realised by existing SaaS, legacy system can be modernised by revising legacy system based on existing SaaS alternatives (Zhao and Zhou, 2014). Additionally, the identified SaaS migration challenges (in **Figure 1** of ***Appendix 1***) have been further grouped into three main issue areas (refer to **Section 3.5**) of cloud computing that should be considered when planning for cloud SaaS adoption in enterprises as would be explored in subsequent chapters of this thesis.

Chapter Four

4. Methodology

4.1 Introduction

This chapter introduces the research philosophy, methodology, research design and empirical findings. The objective of each research phase is outlined. Discussions of results and implication of findings, well as observations for future work are also presented. Finally, a summary of research progress to date is provided. For an overview of the research methodology framework employed in this study, please refer to ***Appendix 2***. A constructive programme for the research process is shown in **Figure 4.1**.

4.2 Research Philosophy

In information systems (IS) research, there are a number of different paradigms which provide support for researchers. Such paradigms are usually classified into positivism, critical research and interpretivism (Oates, 2005; Klein & Myers, 2011). However, the approach most widely used in IS research is interpretivism (Walsham, 1995; Klein & Myers, 2011; Mingers, 2003; Goldkuhl, 2011), partly because it supports researchers in developing deep insights into IS phenomena (Klein & Myers, 1999). In IS and computing research, interpretivism is seen as "understanding the social context of an IS – i.e. the social processes by which it is developed and construed by people and through which it influences, and is influenced by, its social setting" (Oates, 2005, p. 292), with the aim of finding new meanings of multiple realities (de Villiers, 2005).

Therefore, interpretivism tries to investigate the social context of an IS and to determine what factors influence users of such a system. These are elements which are difficult to investigate within the positivist paradigm (Myers & Avison, 2002; Goldkuhl, 2011). Silverman (1998) argued that the interpretivist approach could support understanding the process of organisational change. The current research is built on a study of the factors including technical, security, organisational, economic and regulatory which influence a cloud lock-in situation and/or must be taken into account when decisions are made on the migration to, or adoption of cloud computing. Thus, this PhD research philosophy is regarded as falling within the interpretivist paradigm.

- **Research Approach**

Research methods can be classified into three main categories: quantitative, qualitative and mixed method research (Bryman, 2012). Quantitative research is defined as "a research strategy that emphasises quantification in the collection and analysis of data" (Bryman, 2012, p. 35), and is associated with the positivist paradigm, while qualitative research uses an explorative approach to

improve the understanding of social or human problems (Creswell, 2009, 2007) and to understand phenomena (Green & Browne, 2005). There is a long-standing history of using qualitative approaches in IS research (Myers, 1997; Goldkuhl, 2011). Data collection methods for qualitative research are designed to explore issues and elicit opinions and explore the ambiguity of the phenomena and are appropriate for an interpretivist approach. Bryman (2012) noted that quantitative approaches are used to test theory (deductive) while qualitative approaches are used to generate theory (inductive).

This PhD research study adopts both the inductive method (in Phase 1) and deductive approach (in Phase 2, see **Figure 4.1**) to further investigate the main themes identified from the secondary research to support the development of the proposed cloud migration decision support framework and the supporting strategies to avoid vendor lock-in risks. As this investigation will make use of both qualitative and quantitative data, this research will adopt a mixed method approach combining qualitative and quantitative aspects within a single project (Bryman, 2012). The mixed method approach supports researchers in collecting different types of data by different methods using different sources (Kaplan & Duchon, 1988). Finally, it is argued that using a mixed method approach could increase the robustness of the findings by supporting both richness of the analysis and generalisability of the findings (Kaplan & Duchon, 1988). The following sub-section introduces the research design employed in this study.

- **Research Design**

To explore factors that contribute to a vendor lock-in situation in cloud computing, epistemologically, the study design in this research consists of two distinct phases, as depicted in **Figure 4.1**.

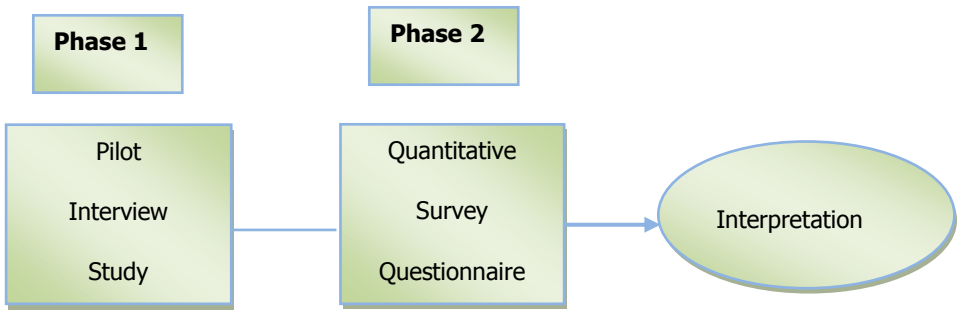


Figure 4.1- Two Phase Exploratory Research Design

Phase 1: For this research, qualitative data has been generated through interview method of data collection. To collect substantial and in-depth insight from interviewees, qualitative interviewing will involve an informal conversational interview, where open-ended questions are asked. This informal interview is considered a pilot phase for the researcher.

Phase 2: Quantitative data from large number of respondents has been accumulated using survey data collection technique via questionnaire. The questionnaire will consist of several questions that the respondent should answer in a set format. The structure of questions in the questionnaire consists of a mix between open-ended, multiple-choice and close-ended questions. To ensure author achieves an effective response rate, questionnaire will be administered by: (a) Face-to-face questionnaire administration, and (b) computerized questionnaire administration using Survey Monkey tool. Additionally, the development of the migration framework will be proposed, tested and evaluated using in this phase of the research study. For further discussion and description of our framework, please refer to Chapter 5.

- **Rationale for the Chosen Research Design**

Research is simply a scientific, methodological way of finding answers to questions, and the type of research design used is based on the purposes of the study. This study seeks to contribute substantially to the development of prescriptive strategies to combat cloud lock-in risks by analysing the original data in relation to enterprise organisations who are struggling to migrate and integrate services between different cloud providers and on-premise systems, this is referred to within this thesis as switching difficulties or switching costs.

One of the primary requirements for this research study was to eliminate the gap in the present cloud computing literature as per the vendor lock-in problem, as well as proposing a holistic cloud migration framework. As previously discussed in Section 1.1, while numerous studies cite lock-in as a major inhibitor to cloud computing adoption and migration, yet due to its complexity, intricacy and socio-technical aspects, lack of clarity still pervades within enterprise organisations. Therefore, by implementing the research design in **Figure 4.1** (i.e. mixed-method), author was able to provide a much clearer insight into how complex and intricate migration decisions are made to avoid cloud lock-in risks. Both quantitative and qualitative research approaches were used in this study as well as the evaluation process (refer to *Section 5.11*) simply because they provide complementary information. Moreover, considering that the author's primary aim for combining both research design was to gain insight into the cloud lock-in problem from a business perspective in order to offer suggestions and help, thus the end sought was exploratory and descriptive in nature. Qualitative and quantitative research paradigms seek to explain events from different perspectives, and they are both valid approaches to evaluate the vendor lock-in phenomenon in the cloud computing context. By examining the critical factors of the chosen research design, author was also able to make a more informed choice and enhance both reliability and validity of the study results. In summary, therefore as long as the author recognised and evaluated the flaws in research design when choosing different research methods for this study, any of the specific research methods are valid contributors to scientific knowledge.

4.3 Phase 1: Pilot Interviews

In the pilot study, qualitative data were collected using open-ended interviews with IT practitioners to explore the business-related issues of vendor lock-in affecting cloud adoption. Five participants from different industry sectors and organizations were purposely selected for in-depth interviews. They included a security expert, cloud advisor, IT technician, business end user, and an IT manager. The purpose was to explore the cloud lock-in problems, and explore the prevalence of its dimensions, by gaining a range of insights from different IT professionals. Please refer to ***Appendix 3*** for the interview consent form used prior to collecting qualitative data for this thesis.

Each interview data collected was transcribed verbatim, and the data was analysed using the Nvivo 8 QSR software package for data storage, coding, and theme development (Nvivo QSR, 2015). Due to the participatory and time-consuming nature of this pilot phase, it was deemed important that each interview be given considerable time for analysis. Seven themes emerged in relation to participants' perception of vendor lock-in problem and how this affects their migration and adoption decisions. The themes were; (1) standards, (2) interoperability in the cloud environment, (3) the need for portability, (4) integration challenges, (5) contract exit strategy, (6) data ownership (7) security and privacy issues. The analysis of the responses across the seven themes showed the participants' priority of the themes. Thus, data portability and interoperability concerns were the most discussed theme in relation to vendor lock-in. However, participants were less interested to divulge about the security and contract exit strategies, including data ownership and privacy risks. After the pilot interviews a questionnaire was designed for a survey. The main issues raised at the interviews were incorporated into the questionnaire.

4.4 Phase 2: Survey Questionnaire

The goal of phase 2 was to identify and evaluate the risks and opportunities of vendor lock-in which affect stakeholders' decision-making about adopting cloud solutions. This phase of the research design is based on an online survey tool (Survey Monkey, 2014). Participants were selected and invited by e-mail to participate in the survey. The aim of the survey was an in-depth study of the effect of vendor lock-in in migration of enterprise IT resources to the cloud. As mentioned earlier, the discussions of the pilot study informed the design of the questions in the questionnaire. Please refer to ***Appendix 4*** for a list of questions used in the survey.

4.4.1 Questionnaire Data Collection

The target population mainly consists of large corporations and small to medium-sized enterprises (SMEs) located in the United Kingdom (UK). Participants in the survey varied between IT professionals, managers and decision-makers within their respective business enterprise. A total of

200 companies were invited to participate in the survey. Overall, 114 participants responded and completed the online survey, which constituted a satisfactory response rate of 57 per cent. To supplement for a higher response rate as possible and to avoid skewing the data, a paper-based questionnaire was administered in person to participants at conferences and workshops. 12 completed responses were received, giving a good response rate of 63%. Prior to presenting the findings of the survey, the questionnaire comprised of many questions, however only those which revealed important issues of lock-in are presented and discussed in context. For analysis, **Table 4.1** presents a socio-demographic profile of the companies and participants in the survey. As shown in the table, the samples were slightly dominated by organisations sized between 251 and 500 employees, and majority came from ICT organisations, followed by education, consumer business, public sector and healthcare.

4.4.2 Survey Implementation

In **Figure 4.2**, a clear majority of the respondents were IT managers and CIOs. These are the key people responsible for making buying decisions in the cloud adoption process. This indicates that the role of IT manager in most organisations is still considered paramount as opposed to premise that the advent of cloud computing will make IT management obsolete – that is, some of the existing IT management roles will be moved to cloud providers (Alkhalil et al, 2014). Arguably this is not the case today as pointed by (Cloud Industry Forum, 2014). Cloud computing is a viable deployment model within the context of UK organisations IT strategy, but it is not seen as the only viable model. Most organisations foresee the continued use of on-premise IT alongside cloud-based services for the foreseeable future, evolving into a prevalence of hybrid IT estates. In addition, a recent cloud Industry forum (2016), research found that final decision-making about the move to cloud computing falls to the head of IT/CIO in around six in ten organisations, although a range of internal stakeholders are involved in the decision-making process.

Table 4.1 Socio-Demographic profile of participant organisation

Organisation Size	**Percentage**
1 – 24	7%
25 – 50	12%
51 – 250	28%
251 – 500	39%
Over 501 Employees	14%
Total:	100 %
Industry Sector	**Percentage**
Construction sector	3.5%
Consumer Business	10.5%
Education sector	15.8%
Financial services	4.4%
ICT services	17.5%
Production & Manufacturing	7.0%
Public sector & Healthcare	11.4%
Services industry	10.5%
Other	19.3%
Total:	100

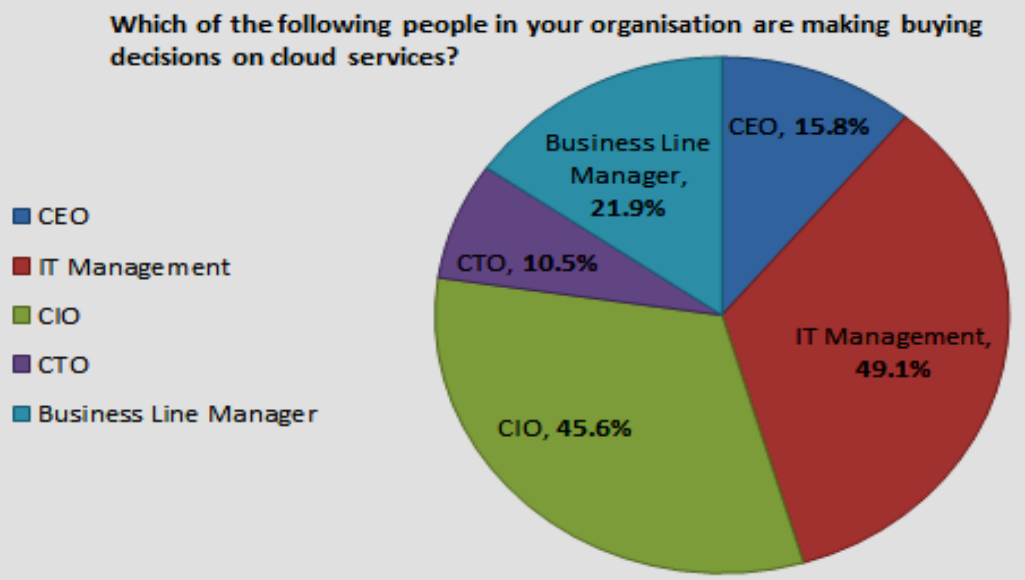


Figure 4.2- Sample profile of participants

4.5 Empirical Findings

The analysis of the results show over 49% of top level IT managers influence the decisions for adopting cloud services **(Figure 4.2)**. This confirms that cloud computing adoption in the UK is a viable IT deployment model. Moreover, more than half (50.9%) of the organisations polled in the study are already using cloud services for at least one application domain within their organisation. The higher majority (69%) utilise a combination of cloud services and internally owned applications (i.e. hybrid IT) for organisation's needs **(Figure 4.3)**.

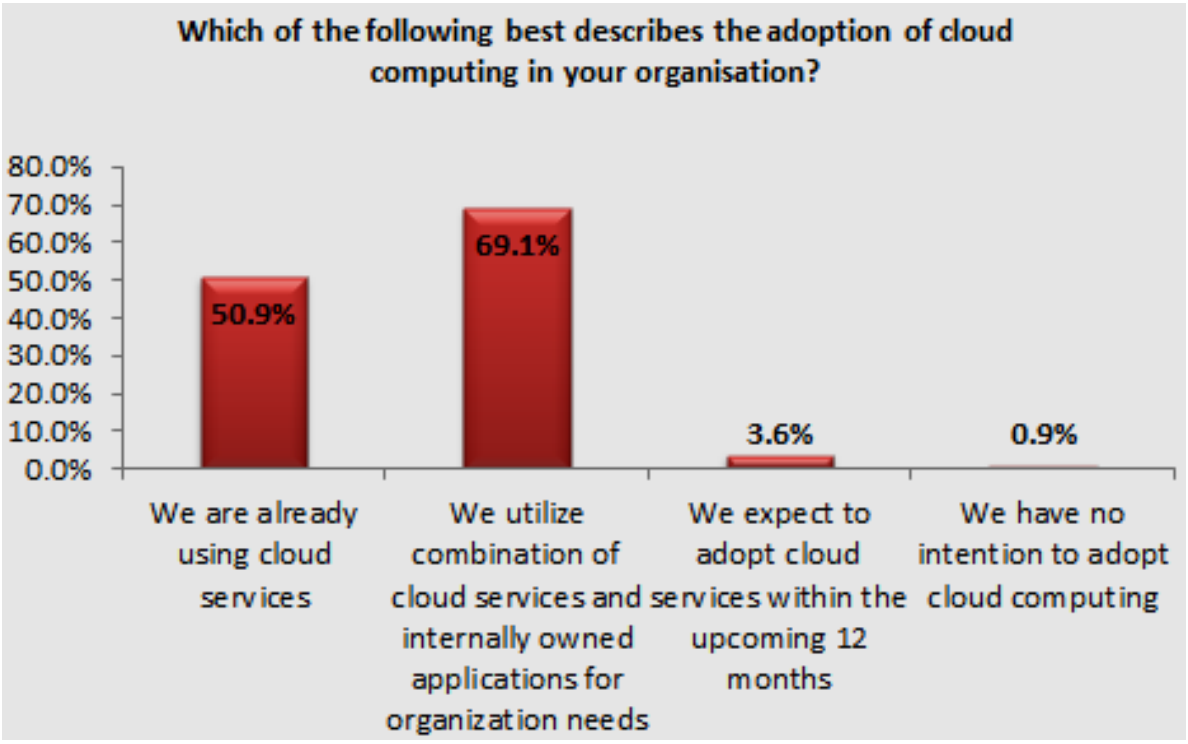


Figure 4.3- Cloud Adoption Maturity in UK

4.5.1 Adoption of Cloud Computing by UK Businesses

The survey affirms that the concept of using cloud computing services to address business IT needs has established a mainstream deployment across organisations of various sizes. To further substantiate this matter, interestingly about 36% of participants admit to using a hybrid (public and private) cloud deployment model as opposed to a private cloud. Only 46% of UK firms participated in the survey use public cloud services, despite the associated security risks (**Figure 4.4**). The rate of adoption has been motivated by numerous factors that are key indicators for effective cloud deployment decision. The most cited reasons for adopting cloud computing includes better scalability of IT resources (45.9%), collaboration (40.5%), cost savings (39.6%) and increased flexibility (36.9%). This suggests that organisations are allured to utilising cloud services due to the perceived business benefits of cost savings, IT flexibility and business agility.

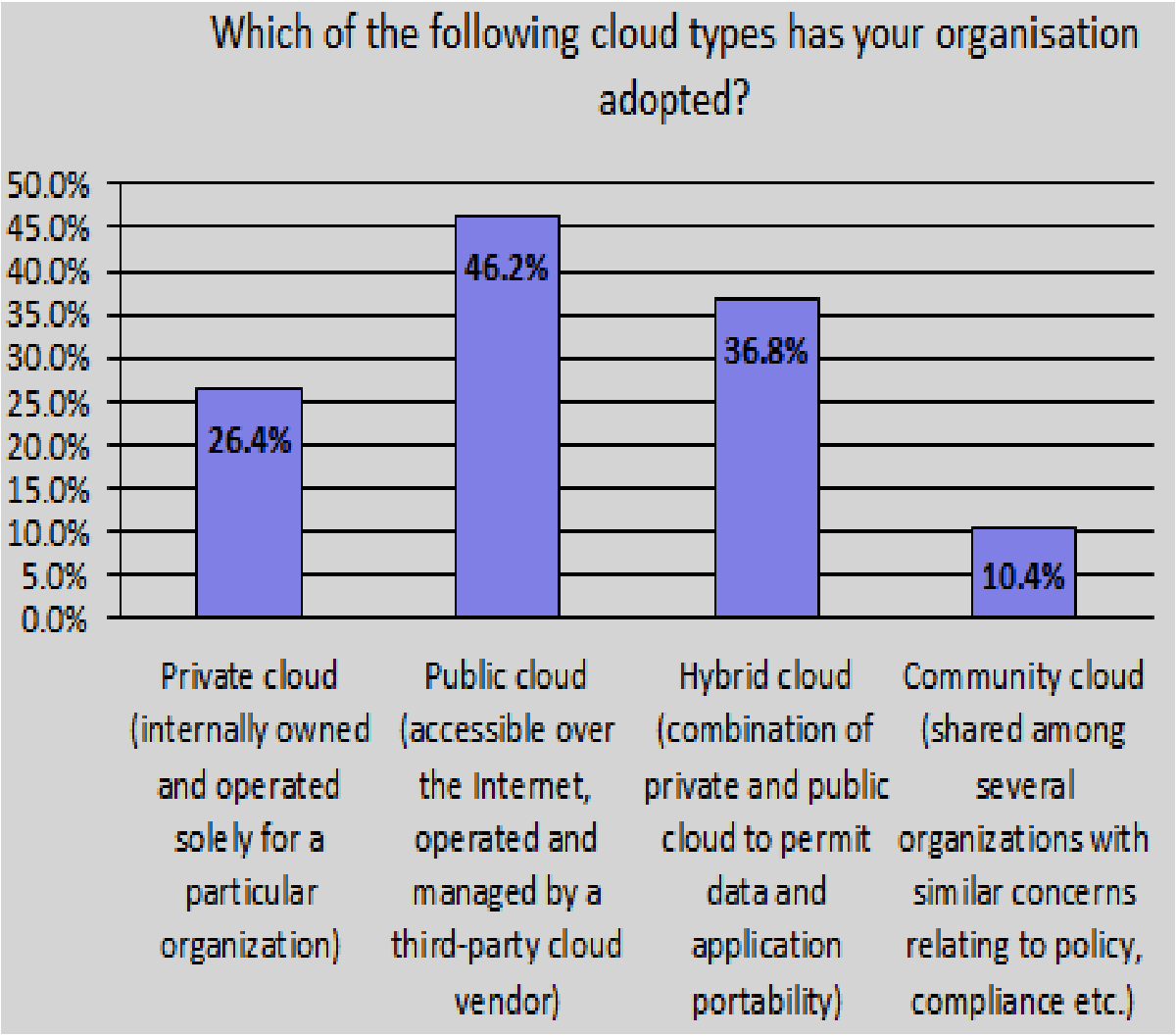


Figure 4.4- Service Deployed Models

4.5.2 The Business Benefits of Cloud Migration

In addition to the reasons for why the cloud model has achieved a mainstream deployment status across UK organisations, defining the actual benefits of cloud computing is critical to further our understanding of the motivations to migrate to cloud-based services. As shown in **Figure 4.5**, the majority business respondents identified capacity and scalability (70.3%), increased collaboration, availability, geography and mobility as achieved benefits for migration. However, when further analysis is undertaken, from a business stance, outside organisations sized between 0–250, the three most important realised benefits reported by participants include reduced infrastructure cost, ubiquity, and increased collaboration respectively. This indicates that the business benefits of migrating to the cloud vary across different organisation sizes and industry verticals. Moreover, the results also show slight difference between the motivations for adoption and the actual benefits realised from using cloud services.

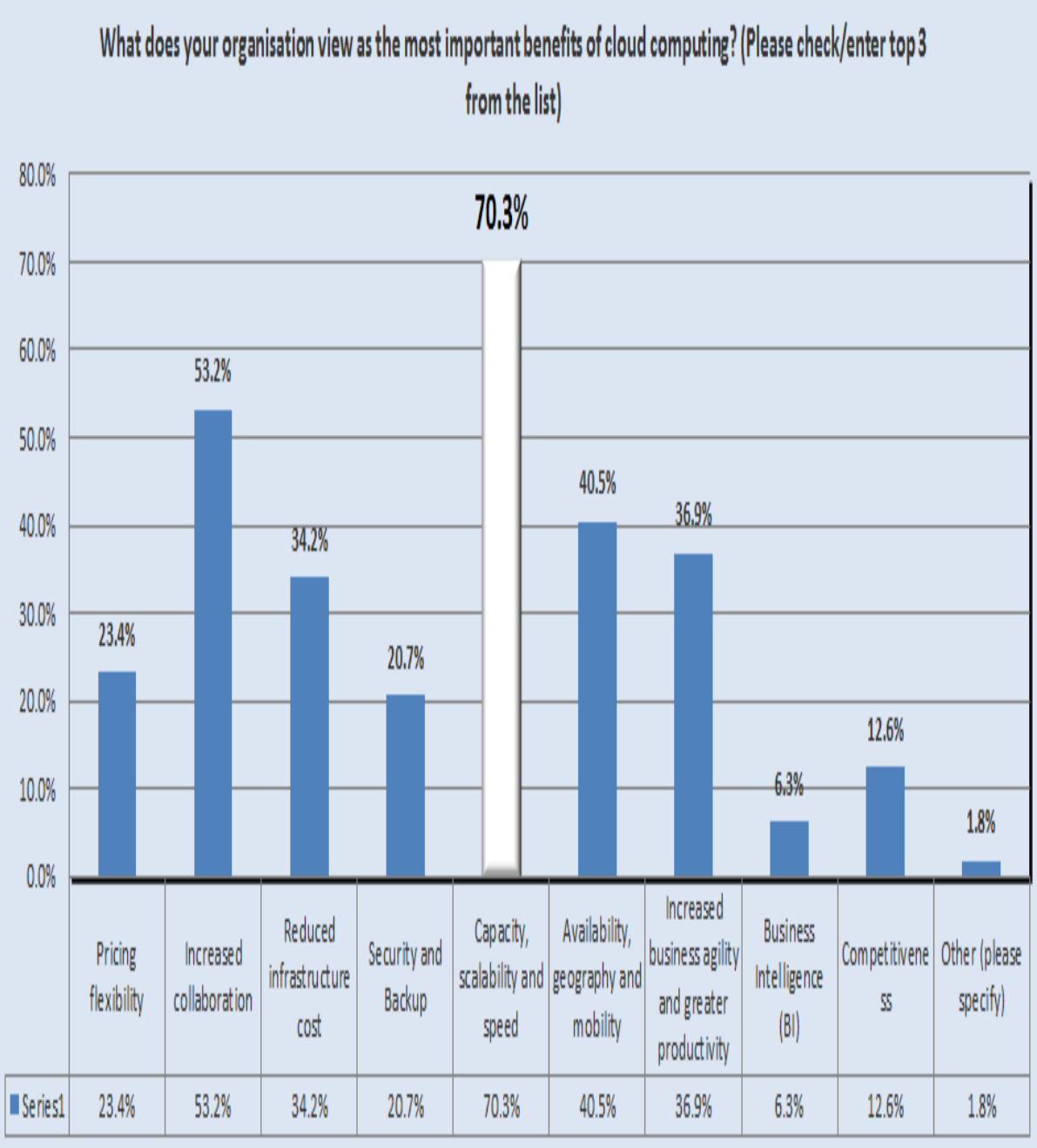


Figure 4.5- Benefits of Cloud computing to UK Enterprises

4.5.3 Challenges to Cloud Implementation for UK Businesses

To identify the factors that impact cloud implementation and purchasing decisions, this study explored "what are the greatest barriers for implementing cloud computing in your organisation? **Figure 4.6** shows the barriers identified by participants. Respondents identified system and data security risks, loss of control and over dependence on a single cloud provider (35.1%) as core existing barriers to future cloud implementation. To confer from this result, security is still a major concern for UK businesses in implementing cloud solutions. In fact, this is due to lack of trust often associated to

worries about loss of control (i.e. in terms of system availability and business continuity risks), as indicated by (48.6%) participants in the study. For instance, some organisations are worried about security within the cloud (i.e. data centres), while others feel that moving data into different geographies could have regulatory (compliance) implications. For example, regarding whether geographical location matter to where organisations' data was required to be stored, 64% of respondents in the survey confirmed location mattered somewhat, 18 per cent claimed location completely mattered. Moreover, the preference of organisations (15%) who believed location did not matter at all can be explained by company's specific need regarding location of data centres and security of cloud storage (refer to **Figure 4.7**). In cloud computing, data protection and data confidentiality are top concerns in respect of data protection law. Taking the organisations in this study for example, the intrinsic nature of cloud computing can impact on the information governance and compliance with UK legislation. This increases the complexity associated with meeting legal and regulatory requirements for sensitive information.

One of the most legally raised concerns about cloud computing security, for businesses, is that corporate data may be stored and processed in a totally different, and potentially unknown jurisdiction. In part, this is due to loss of control which can incite legal and jurisdictional issues. Taking the organisations in this study for example, the intrinsic nature of cloud computing can impact on the information governance and compliance with UK legislation (JISC, 2011). This increases the complexity associated with meeting legal and regulatory requirements for sensitive information. Besides, another barrier to cloud implementation evident in **Figure 4.6** is legal and regulatory compliance issue (25.2%). Moreover, the findings tie in with a recent study published by KPMG (2013), of which (57%) participants identified "the biggest challenge in managing data security and privacy is compliance". However, regarding systems and data security risks (63.1%), cloud service providers can demonstrate their compliance with, and adherence to, industry-accepted standards for data security and integrity. This will show transparency in practice and capability, and assist the establishment of trust for organisations to implement/deploy their most critical, data-intensive functions and processes in the cloud.

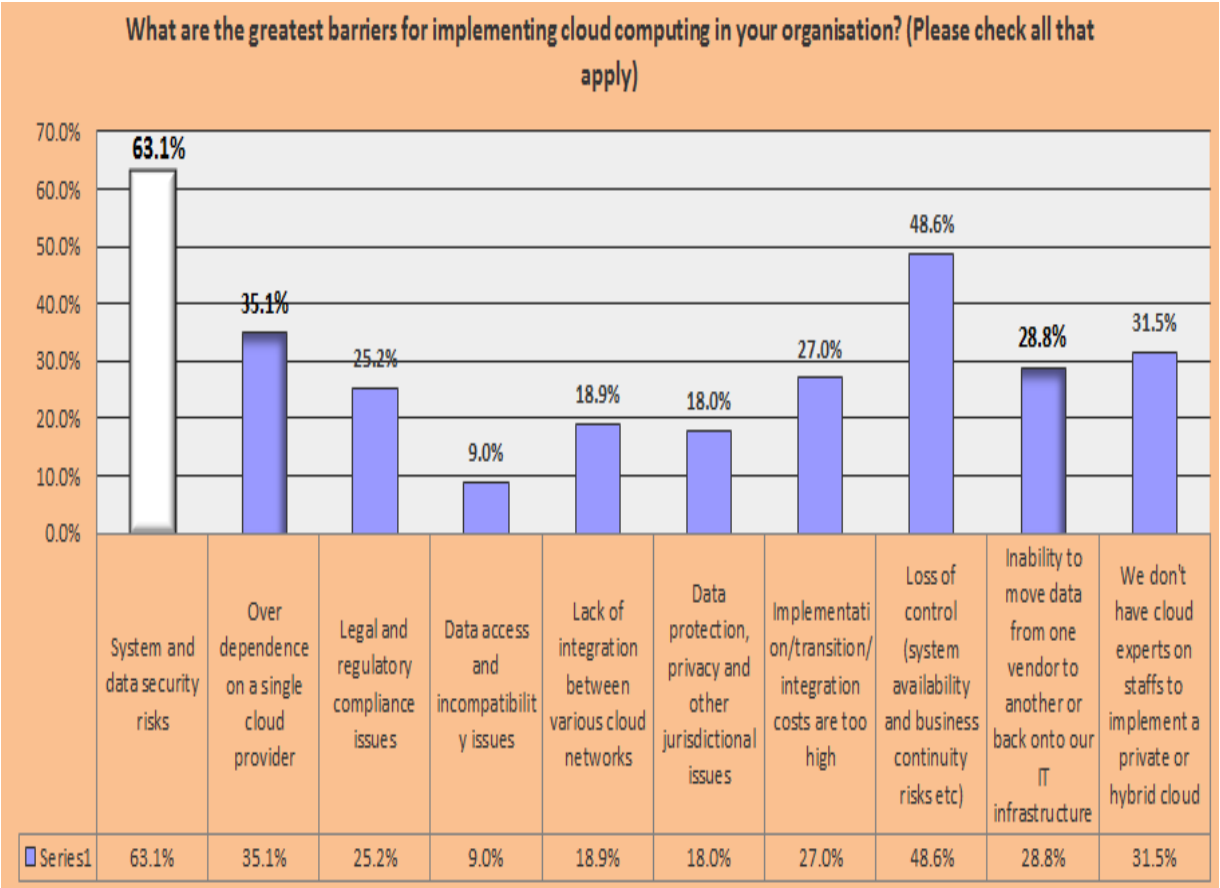


Figure 4.6- Barriers to Cloud Implementation in the UK

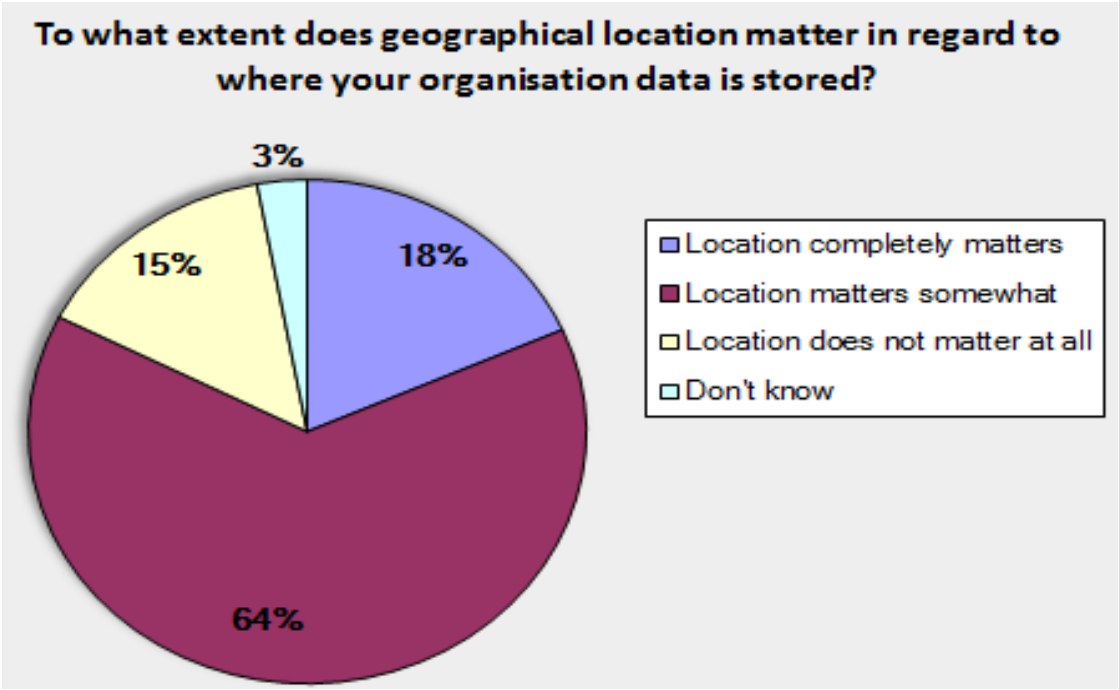


Figure 4.7- Location of data centres raises jurisdictional issues for UK firms

Reflecting on the security and data privacy risks of putting organisations data in cloud storage, **Figure 4.8** shows a clear majority (60.2%) of UK business respondents claiming to be fairly concerned. About 29% admittedly are very concerned, although a lesser minority of businesses are not very concerned at all (10.7%). As well as location, the ubiquitous nature of cloud raises questions about the extent to which data is protected in transit.

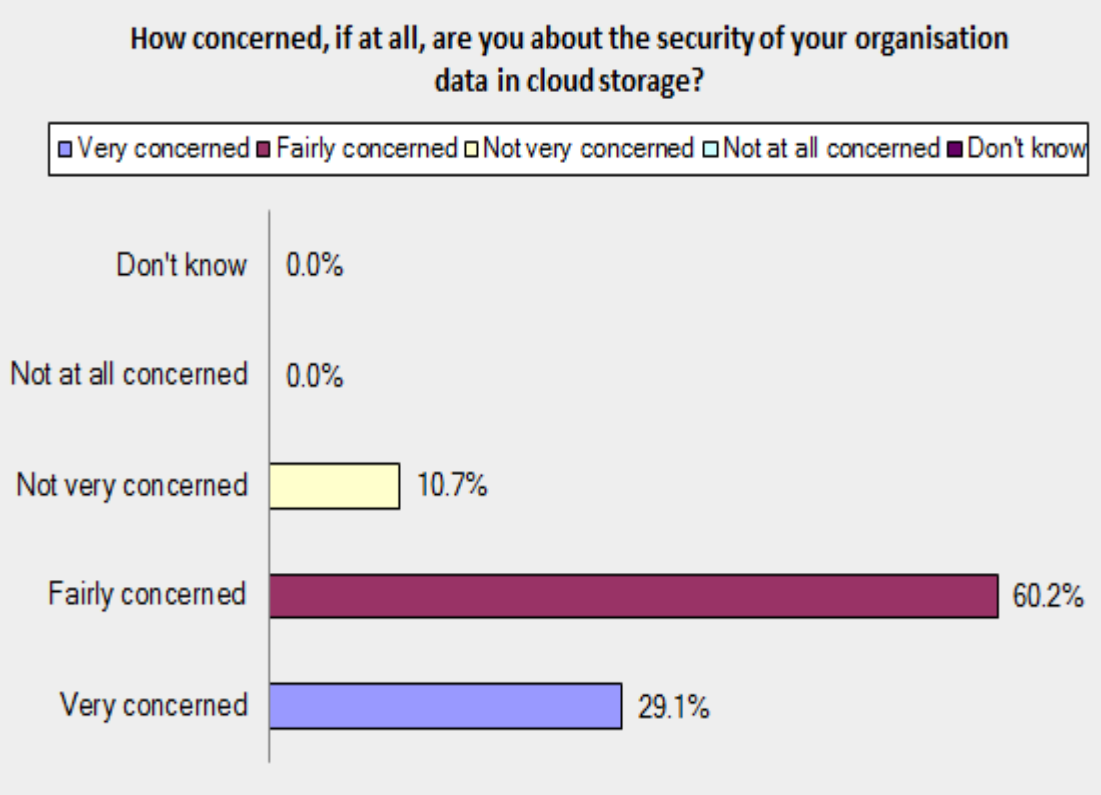


Figure 4.8- Cloud storage security risks affects UK firms

This study also investigates how locations of data centres influence security concerns of UK businesses. Data analysis in **Figure. 4.9** suggests most organisations (3.5%) still consider it safest to have their data stored with a cloud provider located in the UK, whilst (3.36%) preferred data not necessarily be located in the UK but have to be within European Economic Area (EEA). Some organisations, however, still consider it safest to have their data stored on their own hardware in a shared data centre (colocation facility). Overall, interestingly, a vast majority believe locating their corporate data anywhere in the world is unsafe. In other words, the findings indicate that some organisations perhaps operate in a regulated environment where issues with data security, data protection and data privacy laws impact the deployment options available to them. In other words regulatory issues related to security and data privacy risks vary with jurisdiction. This seems unsurprising as data protection law is horizontal rather than vertical, meaning it regulates all sectors, and controllers of personal data remain responsible if processing data in the cloud (Hon et al. 2012).

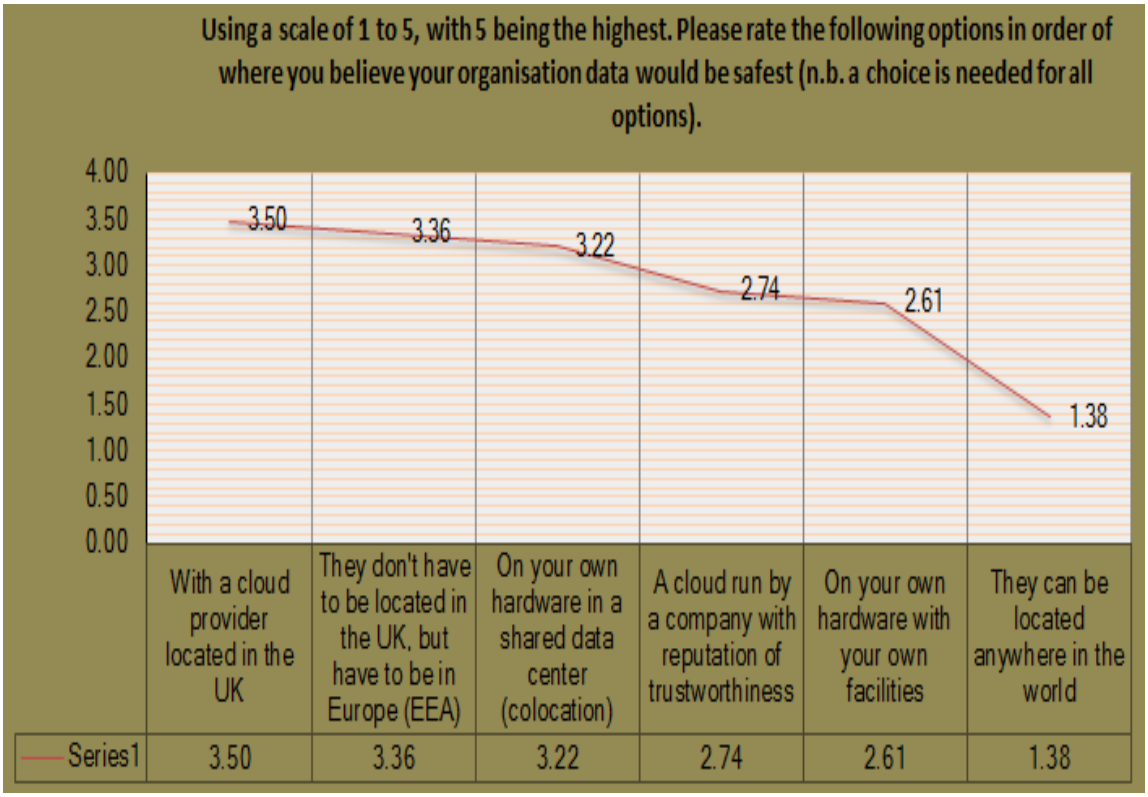


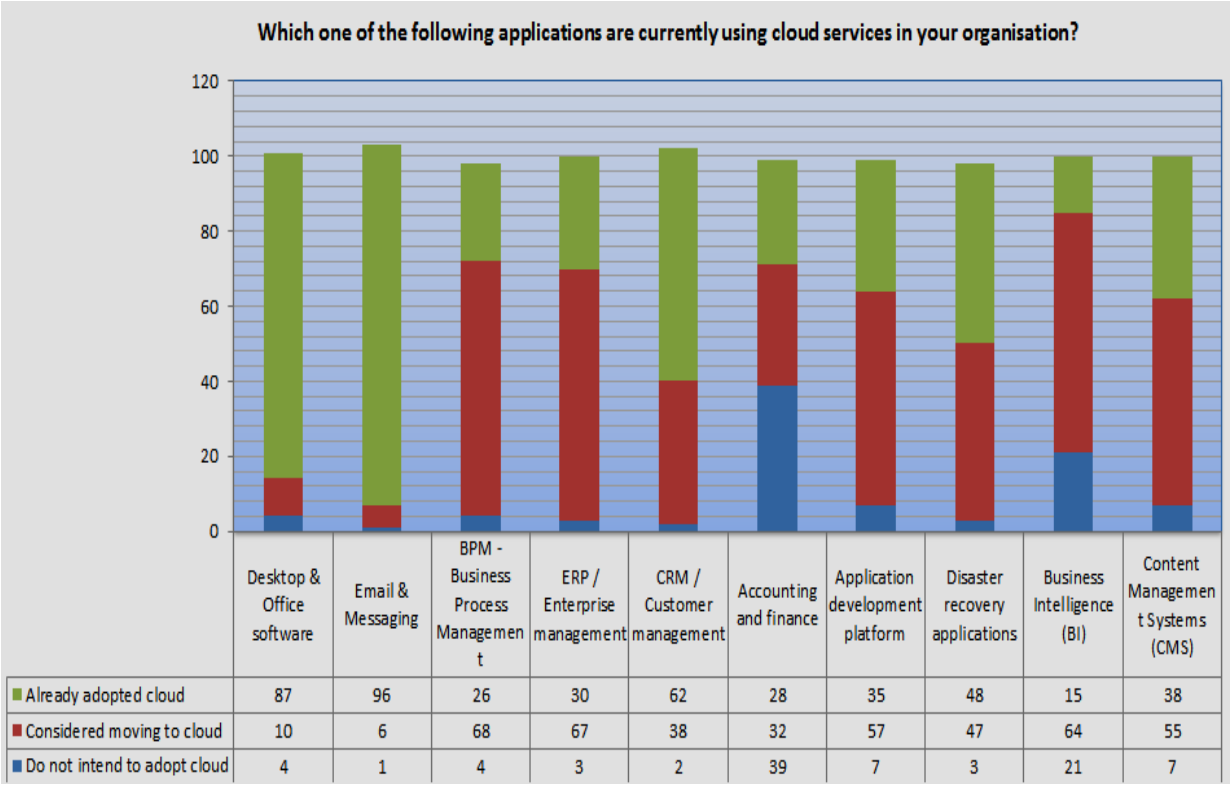
Figure 4.9- Enterprises prefer corporate data stored within the UK and EEA

With regards to **Figure 4.9**, the result suggests businesses are not concerned about the co-location data centre within the country so much as global data centres. Verifying that data are processed in data centres claimed by cloud providers is difficult, technically. Admittedly, trust is a hard thing to establish in cloud computing, nevertheless cloud providers may help increase consumer trust by enhancing transparency in terms of location of data centres, as well as assisting businesses with legal compliance as they move to the cloud. Finally, in terms of security and data privacy risks, clarity and scope of the operating environment are essential factors to consider in making confident and effective deployment decisions. Thus, the emerging challenge for business stakeholders' in their respective organisations is to ensure good governance and security compliance for effective delivery across a range of in-house and cloud-based services. Education is required in this aspect, to reassure and build confidence in the cloud business model – seeing as businesses still lack sufficient knowledge about cloud-based solutions and services.

4.5.4 Cloud Application Usage and Service Adoption among UK Organisations

To identify the opportunities which may affect stakeholders' and decisions for or against cloud migration, this study polled decision-makers to see which applications have adopted cloud services, which they considered moving to the cloud and which, for whatever reason, they intend not to adopt the cloud model. The findings presented herein continue to validate cloud solutions as being pervasive

across UK organisations and industry sectors. The results in **Figure 4.10** suggest that general purpose applications suit such as email and messaging, desktop and office software and customer relationship management applications have all adopted the cloud delivery model. It should be noted that the widespread and reckless sign of adoption could pose significant risks, seeing as the cloud computing era is still evolving. This is further reinforced by respondents who consider moving business process management (68%), enterprise management (67%), and business intelligence applications (64%) respectively to the cloud. This move certainly reflects the impact that the cloud has on the delivery and use of enterprise software applications, as identified by respondents.



	Desktop & Office software	Email & Messaging	BPM - Business Process Management	ERP / Enterprise management	CRM / Customer management	Accounting and finance	Application development platform	Disaster recovery applications	Business Intelligence (BI)	Content Management Systems (CMS)
Already adopted cloud	87	96	26	30	62	28	35	48	15	38
Considered moving to cloud	10	6	68	67	38	32	57	47	64	55
Do not intend to adopt cloud	4	1	4	3	2	39	7	3	21	7

Figure 4.10- Cloud-based CRM and ERP Service Adoption Rates Soar

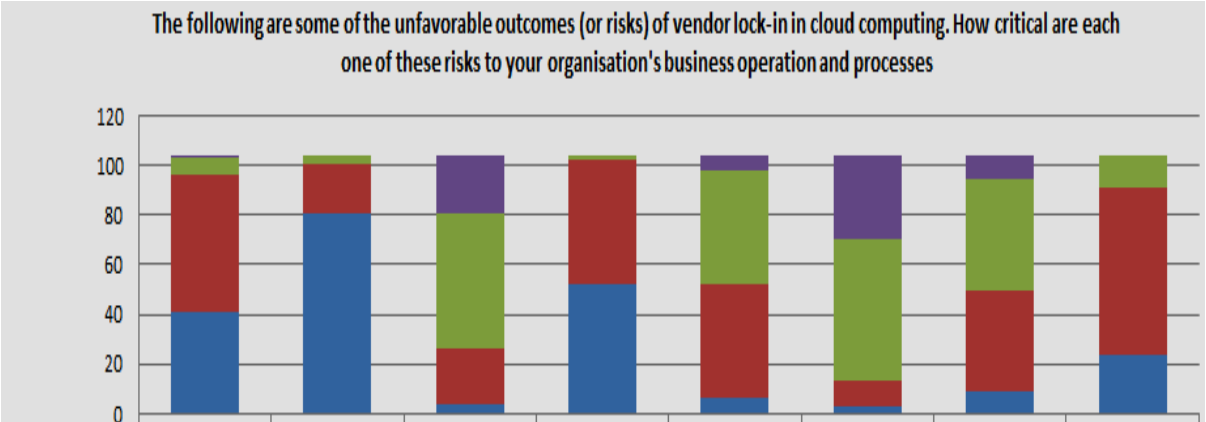
In **Figure 4.10**, the one application identified by most business respondents as not suitable for cloud deployment is accounting and finance (39%), perhaps due to data security concerns. Moreover, further data analysis in cloud adoption rate across organisations, realised that larger enterprises find disaster recovery, (ERP) and business process management applications (BPM) as best fit for cloud migration. Although for smaller enterprises, the adoption of (non-mission critical) cloud-based applications mirrors their use of email messaging, desktop hosting and Customer Relationship Management (CRM) applications for collaboration. Remarkably, the lower cost and flexibility that cloud-based applications offer is ideal for small businesses, as they are agile and often run with teams that are spread over wide geographical regions. These applications are better suited for online delivery (Dubey and Wagle, 2007).

4.5.5 Vendor Lock-in Concerns and Challenges in Cloud Migration

As cloud computing adoption rate soars across the UK market, the risks of vendor lock-in is also prevalent. How lock-in critically affects an organisations' business application and operation in the cloud cannot be overemphasized or underestimated. For example, **Figure 4.11** paints a clear admonitory picture of how UK businesses rate the risks of vendor lock-in against the decision to migrate/adopt cloud services. UK businesses are concerned with data breach and cyber-attack, failure to meet agreed service levels and having corporate data locked-in to a single cloud provider. The risks (in **Figure 4.11**) were identified from the initial pilot interviews and from the literature (Satzger et al. 2013; Binz et al. 2012; Open Group, 2011; Petcu et al. 2013; Opara-Martins et al. 2014). Moreover, the following risks (i.e. inability to move data and applications in/out of cloud environments, data ownership and cyber breaches) in **Figure 4.11** were critical themes that emerged from the unstructured interviews with IT practitioners. The overall results in **Figure 4.11**, highlights that besides the risks of data breach and cyber-attack, or failure to meet agreed service levels, UK businesses are also concerned about having corporate data locked-in to a single cloud provider. These concerns affect the wider business functions where an enterprise is using cloud to perform essential business activities to keep operations running.

Based on the analysis drawn from **Figure 4.11**, while cloud applications may offer outstanding value in terms of multitenant features and functionalities, they also introduce several portability, integration, and interoperability challenges that hinder enterprises' decisions for or against cloud adoption. The first challenge is that, many organisations have different systems and applications that might use different technologies, protocols, applications and devices distributed across a network (Mahmood and Hill, 2011; IBM, 2012). In such heterogeneous environments, information can come from many places — such as transactions, operational, document repositories and external information sources in many formats, including data, content and streaming information (IBM, 2012). In this aspect, lost, inaccurate or incomplete information also can generate high costs and lose of productivity when having to search for information or synchronize data. Moreover, poor data quality can lead to failure of business processes and erroneous decision-making. The second challenge is that most core enterprise applications (such as Customer Relationship Management or CRM, Supply Chain Management or SCM and Enterprise Resource Planning or ERP systems) are being packaged to the cloud in a Software-as-a-Service (SaaS) model, and delivered to companies as point solutions that service only one Line of Business (LoB). As a result, organisations without a means of synchronizing data between multiple LoBs are at a serious disadvantage in terms of maintaining accurate data, inability to make real-time and information-backed decisions, and difficulty in realizing complete business process automation. Real-time sharing of data and functionality becomes difficult in such distributed computing environment. Finally, since each vendor that provides a cloud solution creates its own application programming interfaces (APIs) to the application, this will complicate

integration efforts for companies of all sizes (small or large) and locations as they struggle to understand and then manage these unique application interfaces in an interoperable way, and integrate applications from cloud to cloud and cloud to on-premise systems. Therefore, as enterprise environments are becoming increasingly distributed and heterogeneous, there is a need to integrate between disparate systems to satisfy business requirements and needs. In this direction, author argues that interoperability is one of the means by which enterprises can achieve such integration (refer to *Section 4.5.7*).



	Having my data locked-in to one cloud provider	Data breach and cyber attack	Costly data migration or data conversion	Failure to provide agreed service/meet service levels	The lack of integration between various cloud networks	Unexpected application re-engineering or business process change	Processing incompatibility and conflicts causing disruption of service	Inability to easily move data and applications in/out of cloud environments
(0) Not critical	1	0	23	0	6	34	9	0
(1) Low	7	3	55	2	46	57	45	13
(2) Moderate	55	20	22	50	46	10	41	67
(3) Critical	41	81	4	52	6	3	9	24

Figure 4.11- The potential for Vendor Lock-in risks in the cloud

4.5.6 Enterprise Perception of Cloud Lock-in Terminology

In the study, it was deemed paramount to first assess participant's current perception of the term "vendor lock-in" in the context of cloud computing. As shown in **Figure 4.12**, only 44% of respondents indicated to have a basic understanding of the term. This indicates that whilst UK organisations are rapidly migrating and adopting cloud services, only a few (3%) had exceptional knowledge. This means the lack of clarity on the problem of vendor lock-in still pervades. In part, this gap of knowledge means that organisations are not aware of the inherent lock-in problem within the cloud environment. However, the result implies that organisations with basic knowledge may not yet have experienced a cloud lock-in situation. A possible explanation for this may be attributed to the immaturity of the cloud computing ecosystem. If organisations' previous experiences in IT are

compatible with the existing information and the infrastructure, then the degree of lock-in introduced by service providers will be consistent with the current knowledge and practice. Hence, to develop a comprehensive understanding to manage the risks associated with lock-in, organisations must first define what the lock-in means to them. This requires mapping and cross-examining the challenges of lock-in with different cloud service types (i.e. infrastructure, platform and software) and deployment models (i.e. public, private or hybrid). Comprehending the term "vendor lock-in" is critical to further our understanding. In agreement with the definition of vendor lock-in provided by Armbrust et al. (2009), in **Table 4.2** as many as 71% of the participants claimed vendor lock-in risks will deter their organisations from adopting more cloud services, although some respondents were unsure.

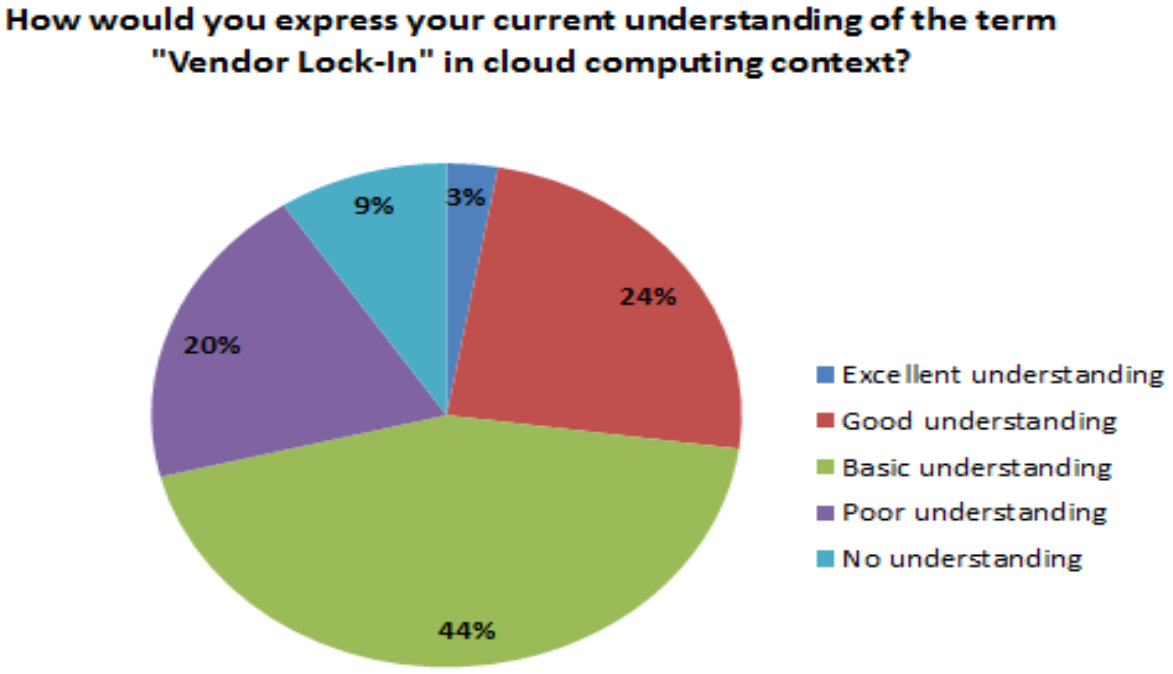


Figure 4.12- UK Business perception of Vendor Lock-in

Table 4.2 Response indicator suggest Lock-in is a deterrent to Cloud migration

Definitely Yes	Possibly Yes	Not Sure	No
9%	71%	11%	9%

4.5.7 Core Risk Factors of Lock-in Impeding Future Cloud Migration and Adoption in UK

To highlight factors which may affect future cloud migration decisions, participants were requested to identify practical challenges of lock-in they encountered when using cloud services. These issues relate to lack of integration points between existing management tools (47.7%), incompatibility issues with on-premise software, and inability to move to another service provider or take data in-house

(**Figure 4.13**). Overall, the results indicate that these challenges closely relate to interoperability and data portability issues prevalent in the cloud environment. Moreover, further results show that a significant majority (76.6%) of participants were unsure of relevant (existing or emerging) standards to support interoperability across clouds and portability of data from one cloud provider to another.

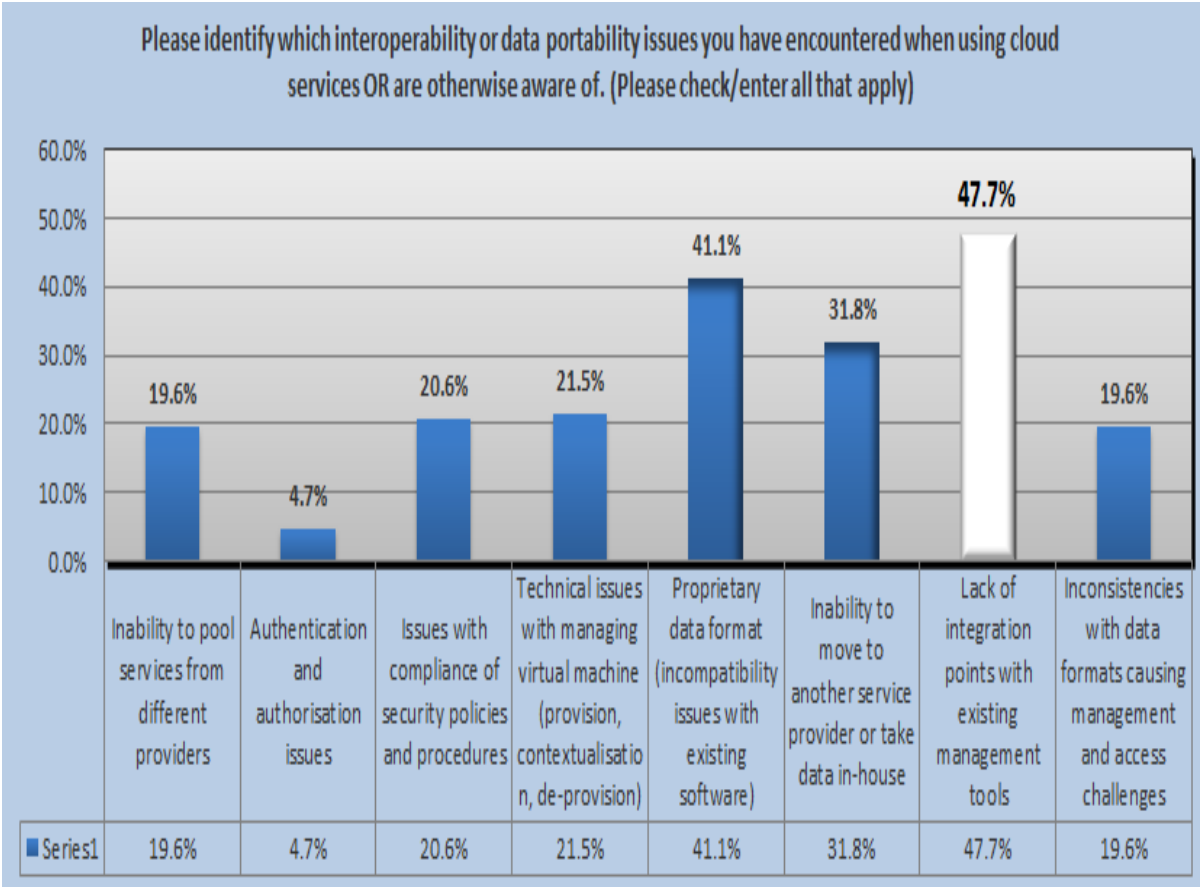


Figure 4.13- Practical challenges of Vendor Lock-in

To confer from **Figure 4.13**, the main challenges associated with cloud lock-in are integration and incompatibility issues, followed by data portability. However, as shown in **Figure 4.14**, when asked to identify best practices to minimize lock-in risks in cloud migration, most business respondents identified the following as top mitigation strategies: (a) making well-informed decisions before selecting vendors and/or signing cloud contracts (66.4%); (b) the need for an open environment for continuous competition between providers in the cloud service market (52.3%); (c) use of standard software components with industry-proven interfaces (39.3%). Equally, in the case of managing the risks of vendor lock-in, it is encouraging to note that respondents expressed by a substantial majority are slightly (39.4%), moderately (33.7%), and quite likely (22.1%) to use a cloud computing risk management framework to manage vendor lock-in risks and compliance requirements effectively. Furthermore, this indicates that UK businesses require effective and efficient strategies to manage lock-in risk(s) prevailing in the cloud ecosystem.

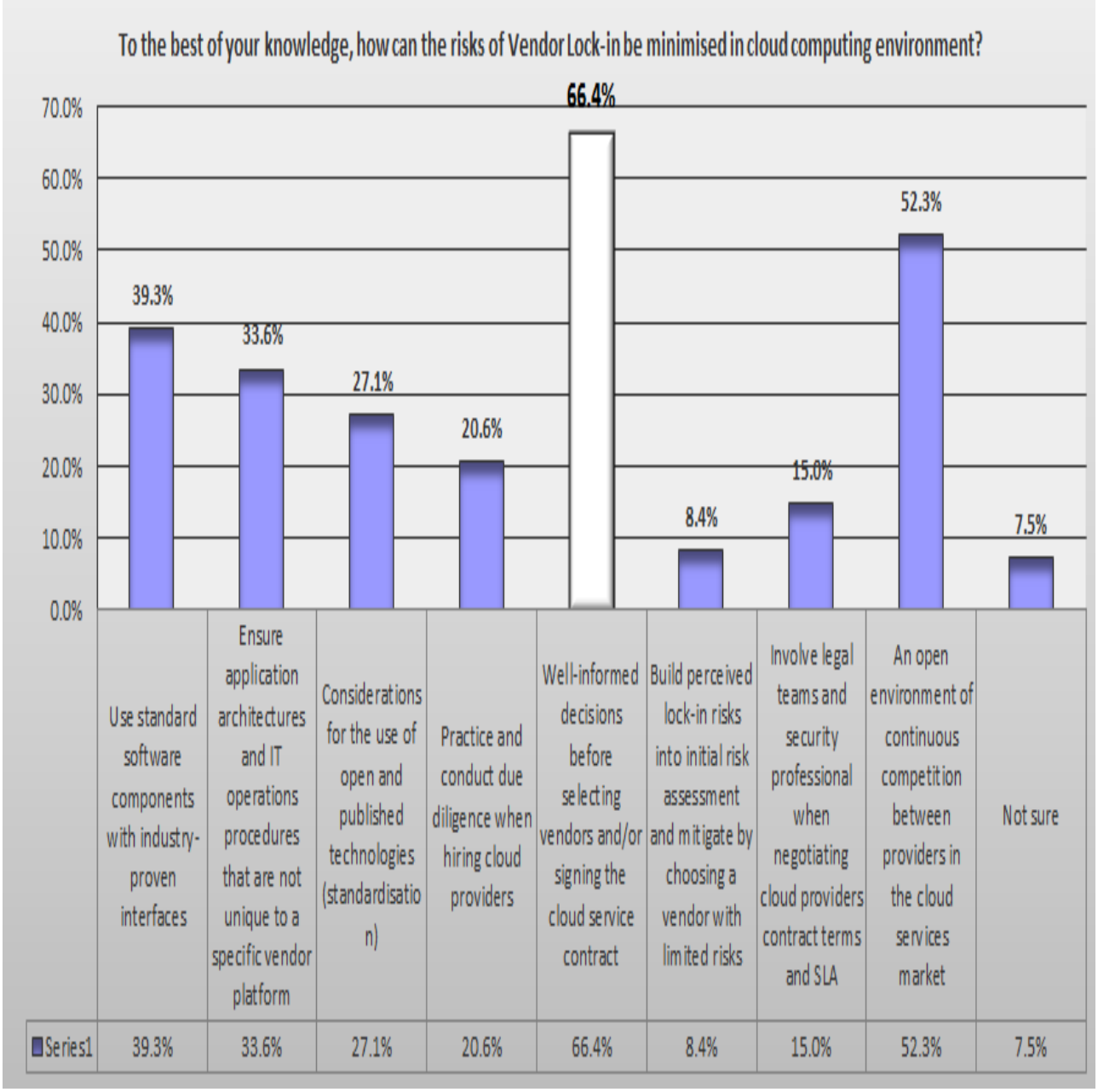


Figure 4.14- Current practice for mitigating Cloud Lock-in risks

4.5.8 Integration Challenges with Cloud Migration

To explore the business rationale for migrating on-premise IT services to the cloud and the integration implications that can occur from sourcing cloud-based services within enterprise environments, this study raised the question "are you considering moving business critical systems (or applications) to the cloud?" The findings in **Figure 4.15** reveals that about 54% of organisations have planned to move one or more business critical systems, while 20% have expected to host critical systems in the cloud. However, only 10% of organisations have implemented critical systems in the cloud environment.

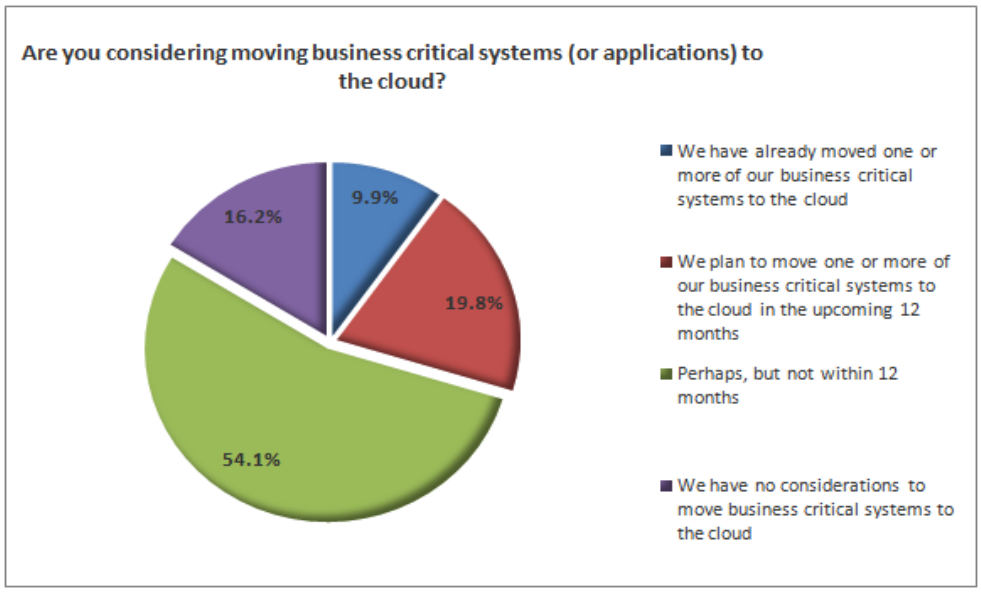


Figure 4.15- Enterprises plan to move core systems to the cloud environment for processing

Underestimating the difficulty associated with integrating between cloud and on-premise is a common pitfall with migrating enterprise systems to the cloud. Cloud adoption will be hampered if there is not a good way to integrate data and applications across clouds (Buyya et al. 2010). Moreover, in (Stravoskoufos, 2013), it is argued that the cost and complexity of developing and maintaining integrations between heterogeneous platforms with disparate interfaces and protocols can easily erase the economic and efficiency gains the cloud delivers. In agreement with the aforesaid, the survey by (Dynamic Market Research, 2013) of business managers around the world on their experiences with cloud-based applications, revealed that companies have abandoned the use of roughly one departmental cloud application a year due to integration problems. In the same study, 54% of respondents acknowledge they have experienced staff downtime due to integration problems, and 75% have had their ability to innovate impaired by poor integration of their cloud applications. This is further sustained with a more recent study by (Snap Logic, 2015), which shows that 43% of companies, with revenues greater than $500 million, noted integration challenges as primary barrier to enterprise cloud application adoption in 2015. Nevertheless, the survey conducted in this paper paints a clear picture on the importance of integrating cloud solutions with on-premise systems. As illustrated in **Figure 4.16**, a clear majority (56%) of respondents indicated that it is very important for their organisations to integrate on-premise IT assets with cloud-based services. This finding suggests organisations with a unique portfolio of IT investments migrating to cloud-based solutions require a mechanism that can easily, quickly and efficiently connect their critical systems to the cloud. It is anticipated that standardization of APIs will significantly help resolve this integration imperative, because it will facilitate development as well as the deployment process – eliminating the necessity of factoring applications to comply with other cloud provider's APIs.

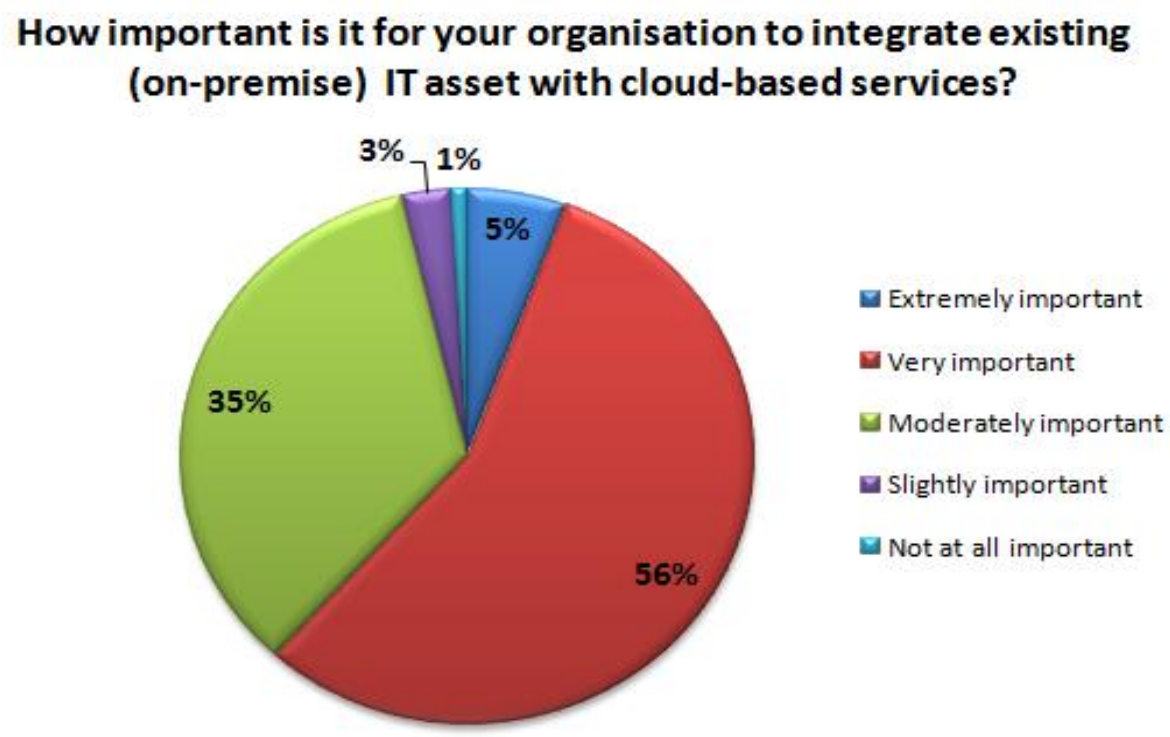


Figure 4.16- Integration is the key to enterprise cloud adoption and migration

A report published by (Dell Boomi, 2015) suggests that businesses currently have the following four primary choices for integrating cloud-based applications with on-premise systems: (a) building a custom-based solution based on the cloud vendor's API, (b) purchasing integration software, (c) subscribing to an integration-as-a-service (IaaS) solution, and (d) engaging professional services or a system integrator. Once a choice has been made, the integration process can be instantiated and implemented in four prominent layers and levels as briefly discussed below.

- **Data Integration**: Data integration deals with moving or federating data between different types of data sources (Chen et al. 2008; Izza, 2009). The main drawback of data integration between cloud and on-premise environment is that the developer will have to understand and maintain the underlying schemas regularly to address any changes (Informatica, 2012). This approach is complex for SaaS applications since the consumers neither have access rights nor control to manipulate the underlying database. The data formats and contents are handled by the service provider, so major data portability considerations are needed. Further, as communication between clouds and on-premise typically has a high latency, this makes synchronization difficult. Also, the two environments may have different access control regimes, complicating the task of moving and integrating data between them. Therefore it is critical that organisations ensure the chosen integration solution is able to synchronize data bidirectional from SaaS to on-premise systems securely without opening the firewalls.

- **Business Logic Integration**: To facilitate integration at this level, the development of a middleware technology is required. Middleware technologies help developers by making the design of distributed cloud solutions less challenging (Bernstein, 1996; Ooi et al. 2006). As an important integration technology, middleware is often used by enterprises to integrate new applications, emerging technologies, and legacy applications. In order for cloud applications to offer the maximum value to users they must provide simple mechanism to import or load external data, export or replicate data for reporting or analysis purposes, and also keep enterprise data synchronized with on-premise applications (Izza, 2009).
- **Communication Layer Integration**: This layer connects the service requestor to the service provider and its underlying solutions platforms realizing the requested service (Open Group, 2011). For example, an enterprise procures a cloud-based application (e.g. CRM) and need to synchronize their master list of customers and other business critical data with their on-premise ERP (e.g. SAP) system in order to meet certain business objectives. Typically, protocols such as HTTP and Internet Inter-ORB Protocol (IIOP) are used to facilitate information exchange among different distributed applications (Benatallah et al. 2008).
- **Presentation Layer Integration**: The integration in this layer mainly focuses on user interface (UI) integration (Daniel et al. 2007). Further work on effective standardization at the presentation layer is required for effective user interface integration to take place. Furthermore, as cloud computing enables new technologies and devices to be introduced into enterprise systems, UI integration poses new challenges associated with various interface types, standards, definitions, and service interfaces. All of these mean that presentation layer integration requires a good understanding of various applications, devices, and enterprise-wide integration requirements.

4.5.9 Interoperability Requirements

Interoperability between clouds is vital for the further development of the cloud ecosystem and market. Interoperability challenges caused by lack of widely accepted standards are what enterprises should wary about when considering cloud integration. Architecting systems to be interoperable and integratable requires one to consider a wide set of standards to implement the solution. To this end, it is therefore important that organisations become aware of appropriate standards and protocols used by cloud providers to support data/application movability, as well as to ease the task of integration. In the light of the advantages of standards in increasing interoperation between cloud and on-premise systems, unfortunately the survey conducted in this paper suggests most enterprises lack a comprehensive understanding in this respect.

This study seeks to identify interoperability requirements for enterprise cloud-based application adoption. However, in the light of the advantages of standards in increasing interoperation

between cloud and on-premise systems, unfortunately the survey conducted in this report suggests most enterprises lack a comprehensive understanding in this respect. As can be drawn from **Figure 4.17**, a significant majority (76.6%) of businesses were unsure of relevant standards to support interoperable cloud implementations. Standards are key to ensure requirements for interoperability, portability, and security, are fully met in the cloud environment. It is therefore important for organisations using cloud computing as an essential part of their business operations, to adopt standards-based products, processes and services. In summary, since integration and interoperability both build upon standards, standardization should be considered as the key to achieve seamless integration and interoperability in a distributed cloud environment. Moreover, due to a number of variables that come into play in a complex cloud solution that involves interoperability capabilities, several case scenarios have been discussed by (Joshi et al. 2014). In a scenario selected, enterprise links in-house capabilities with cloud services. This is done in an effort to highlight key aspects of cloud computing interoperability and current methods for enabling seamless interoperation. This scenario is motivated by the case of a hybrid cloud solution in which the business processes are offered by a public cloud, while other business critical components, and are internally managed by the organization following a private cloud model. In such hybrid environments, enterprises are susceptible to challenges such as maintaining uniform control and transparency over all resources in the distributed environment, whether they are part of public or private cloud resources. However, despite how similar a public and private cloud is built, design and implementation differences will inevitably exist, thus triggering interoperability issues which further complicate the initial integration task.

In the exemplary scenarios above, the main obstacle to achieving a seamless integration is the poor interoperability, since several application components need to interoperate to achieve the business goal. Interoperability challenges come into play when such application components are distributed among clouds. To avoid rewriting the entire application, the cloud services hosting the components must share a compatible API. In this connection, a proper analysis of available APIs of both the in-house system and cloud services is highly required to clearly understand how the integrated system will function and perform during execution. An important aspect to also consider is the migration to and portability among clouds.

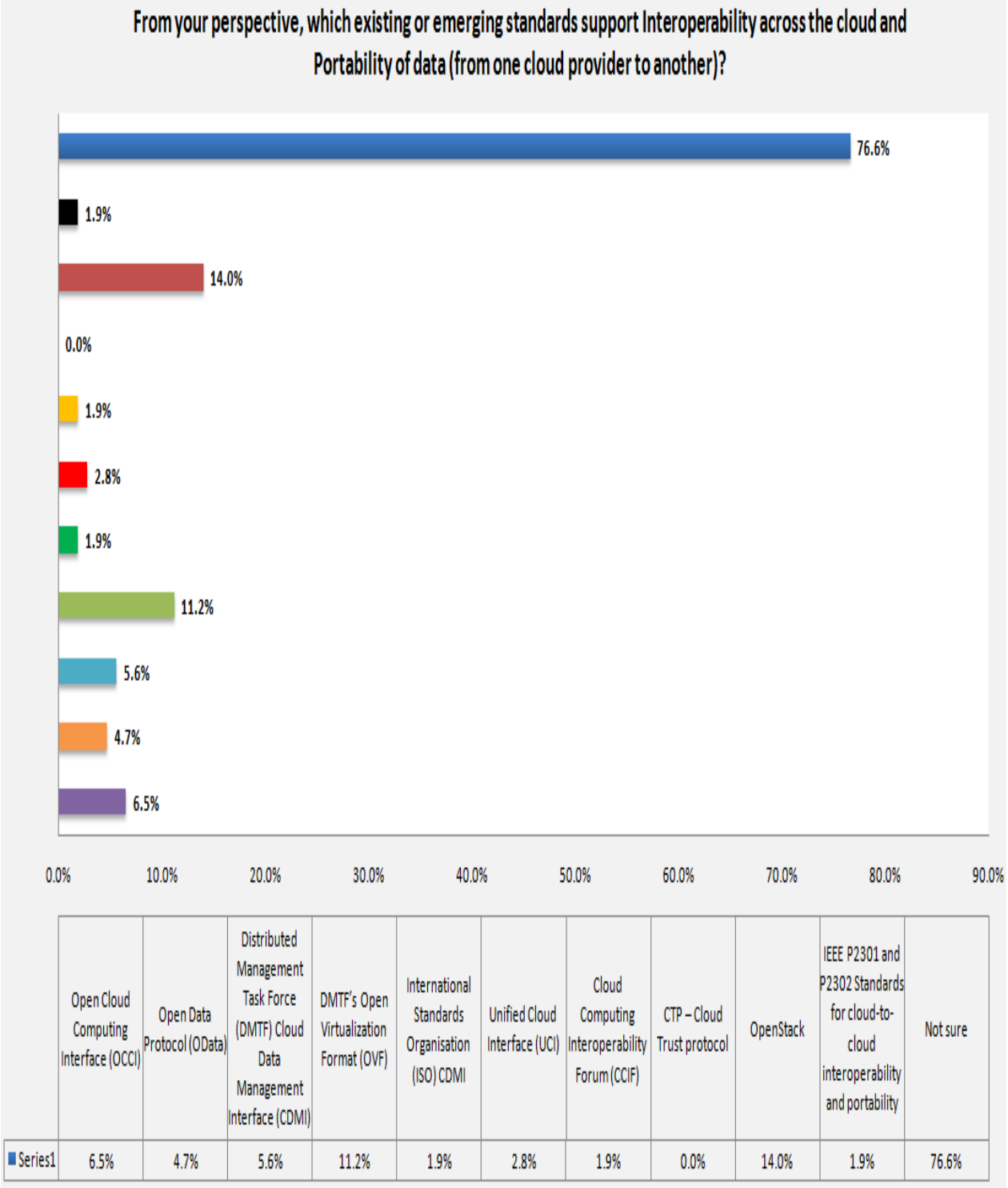


Figure 4.17- Enterprises are unaware of interoperable standards

4.5.10 Contract Lock-in Issues

From a business perspective, there is more than one way to get locked-in to a cloud vendor's system; an often-overlooked method is through a contract. Wang (2012) believes there are three reasons why businesses face vendor lock-in: limited rights and controls for users, ambiguous and ultimately expensive switching costs and vendor complacency. Cloud computing providers can create lock-in

through contractual terms, or through the physical holding of customer's data. In this regard, there is an economic benefit to the vendor in the form of a regular revenue stream, but not so much of business benefits to consumers. From a commercial perspective, this puts the vendor in the position of strength when it comes to renegotiate the commercial terms of agreement. For this reason, it is important not only to review the contract before signing but also negotiate the SLA around crucial elements like data ownership and termination conditions protecting against risks of vendor lock-in. As shown in **Figure 4.18**, just one third of UK businesses in the study had the opportunity to negotiate their cloud service contracts; more than half did not negotiate while a smaller minority were unsure.

However, when conducting further analysis across different organisation it becomes apparent that the rationale for those who negotiated and those who did not covers a wide variety of concerns. Of course, not all businesses may be able to negotiate cloud providers' terms as has been established in the survey's findings. Moreover, as with many commercial agreements much depends on relative bargaining power. Besides, the survey findings in-depth concurs larger organisations from regulated industries had the opportunity to negotiate providers contract terms, unlike small to medium enterprises who are likely to accept the provider's standard terms of service agreement.

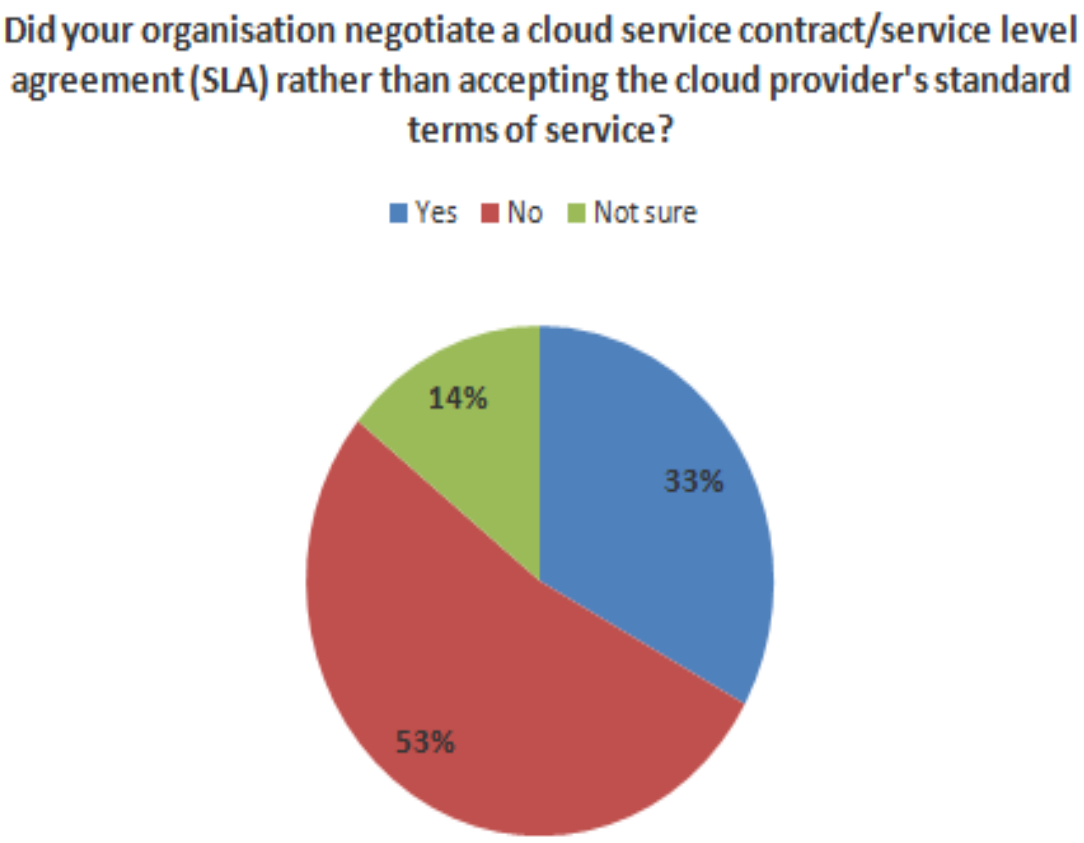


Figure 4.18- Negotiated cloud contracts

Furthermore, to understand how UK organisations plan to minimize vendor lock-in risks through contractual provisions, the survey also explored organisations' cloud exit plans. Surprisingly 24% of businesses surveyed did not have an exit plan, 41% agreed to have an exit strategy in place but with no agreed ownership rights of data that will be stored in the cloud. Only 21% claimed they did not have an exit strategy in case of cloud service termination (**Figure 4.19**).

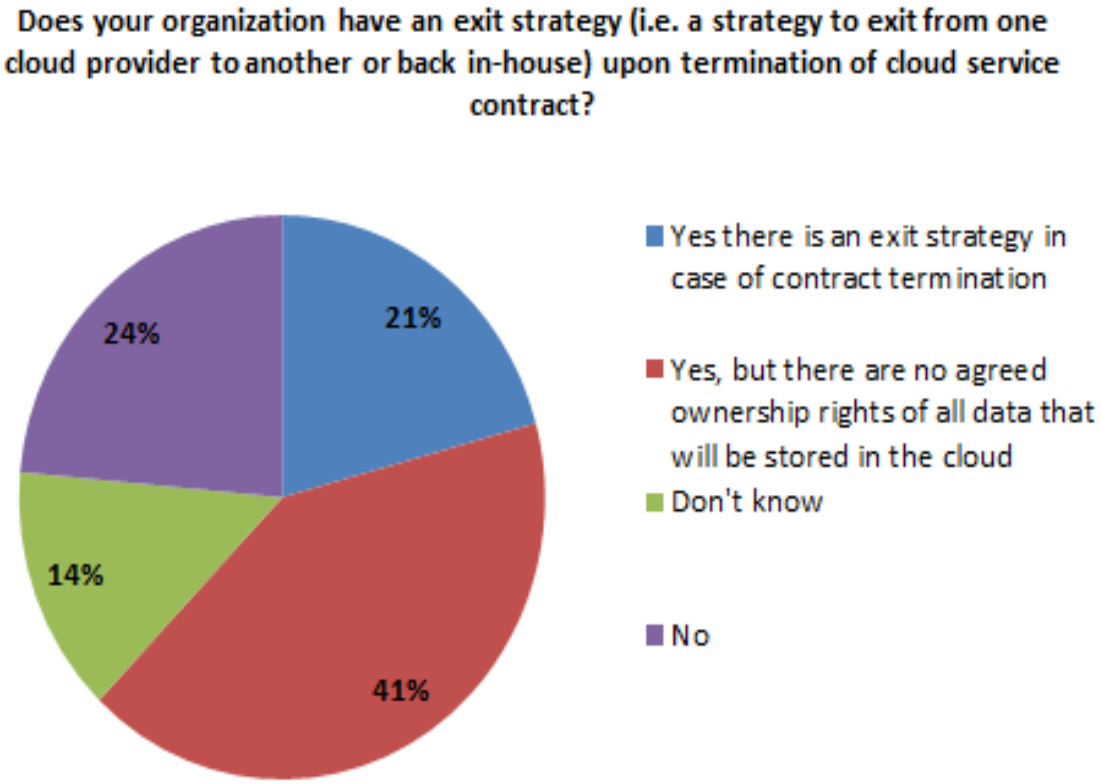


Figure 4.19- Exit strategy is critical in enterprise cloud service contracts

These findings are quite surprising considering what would happen to a company, for instance, if its cloud provider goes out of business. Therefore, it is important to have an exit strategy in place for each cloud type (i.e. private, hybrid etc.) or service model (i.e. IaaS, SaaS, etc.) adopted. This is essential in case of contract termination. In this case, the SLA as well as the terms of conditions should be negotiated around the needs of the business. In this connection, other contractual terms identified by end-user organisations as agreements that meet their risk profiles, compliance obligations, and should be included in the contract/SLA are: right to terminate contract (80.2%), guaranteed service levels (66%), and protection and security of data (refer to **Figure 4.20**). The findings demonstrate that, understanding the most graceful exit strategy for establishing trust should be part of due diligence when vetting potential cloud vendors or service providers. Furthermore, considering the negative impact that the contractual issues identified can have on a business, when using any cloud-based solution, it is important to ensure tools or processes are in place that can facilitate consumers to extract, access, and interchange data if such a need arises.

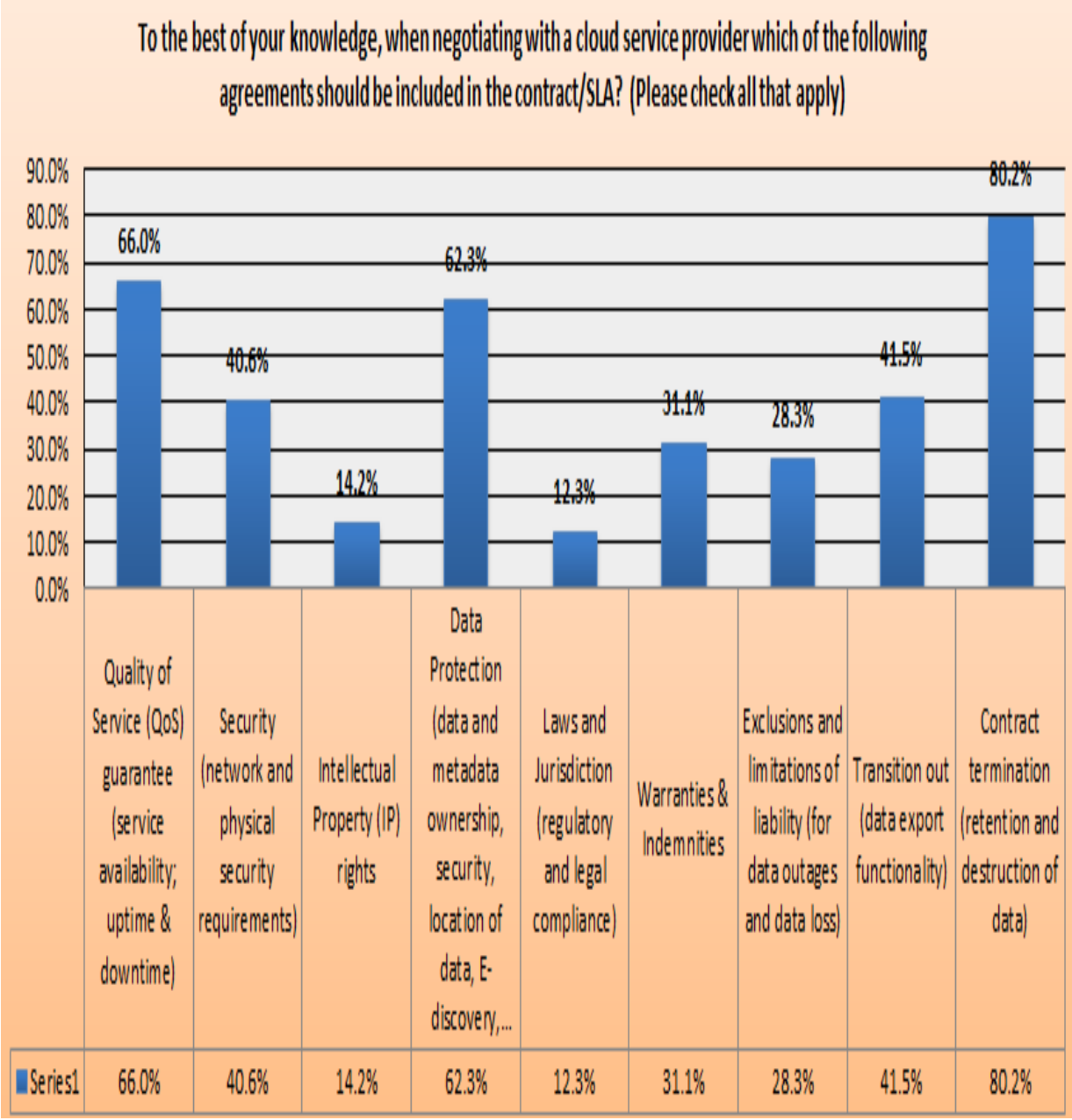


Figure 4.20- Contract terms that generated most negotiation

4.6 Analysis and Discussions

4.6.1 Business Strategies for Avoiding Vendor Lock-in

This section summarises both the desires and experiences of the participants who contributed to this study regarding the cloud lock-in problem. Moreover, this section presents strategic approaches for mitigating the risks and challenges of lock-in in cloud migration.

4.6.2 Awareness of the Commonalities among Cloud providers

To refer to the first research question of interest to business adopters stated in *Section 1.1*. UK business decision makers are rightly concerned about the risks of being locked into a single cloud service provider and the implications of such a risk including not having a clear exit strategy. There is a need for these organisations to understand what the exit strategy looks like, even if it is unlikely that they will exit soon – besides, no company would want to buy into a service where they feel they had no alternative provider. In this connection, one possible strategy will require decision-makers to possess a comprehensive understanding of the heterogeneity that exist between cloud semantics and the cloud interfaces. This often requires an awareness of the commonalities (i.e. complexities and dependencies) among services offered by cloud providers and standards used. By clearly understanding this, organisations will realise how the clouds lose structure can affect data/application movability and security of data sent in it. This can be done by having an in-depth understanding of how data and application components are handled and transmitted in the cloud environment. When this is well understood, and harnessed (at pre-contractual phase), the benefits to the organisations become apparent (at post migration phase). Additionally, enterprises can be more interoperable and avoid vendor lock-in strategically by selecting vendors, platforms, or services that support more standards and protocols (as further discussed below in *Section 5.1.3*). This is essentially important in the vendor selection process as it enables organisations to maintain a favourable mix of cloud providers and internal support. These strategies can help organisations to form a plan for an efficient and effective migration and adoption process. Having a clear understanding of the disparity between cloud semantics and service interfaces offered by different cloud vendors can help significantly to reduce the effects of vendor lock-in.

Substantial training and stakeholder engagement is necessary to develop an understanding and agree solutions on specific lock-in concerns (Premkumar and Michael, 1995; Eder and Igbaria, 2001; Daylami et al., 2005). Otherwise, cloud services offered to enterprises may not be properly assessed for potential lock-in risks before decisions are made to use the service (Binz et al. 2012). Moreover, the results in **Figure 4.6** indicate a general lack of understanding and awareness of lock-in problem in the cloud. The low response gained from participants who identified over dependence on a single cloud provider (35.1%) and difficulty to move data back in-house or across to a different cloud

provider (28.8%) platform illustrates the unawareness of practitioners on the potential effect of cloud lock-in problem. To infer from this result, it appears the risk of dependency is a more significant barrier than data lock-in. This seems counter intuitive considering the practical challenges associated with the data lock-in when extending the use of cloud in the enterprise. However, the probable explanation is that presently most organisations are too reliant on cloud providers for operational and technical support (Dutta et al. 2013), thus they fail to fully prepare to deal with unexpected and undesirable data lock-in issues in the cloud (referring to **Figure 4.13**). As pointed out by Bradshaw et al. (2012), lock-in will become more of an issue as the cloud computing market matures. In agreement, Lipton in (2013), admits that the complexity and cost of switching (or porting) a cloud service to a different provider is often under-appreciated until it is too late. Therefore, it can be claimed that if corporate data is not locked-in moving to another cloud provider is just a matter of enduring a switching cost. Such cost can be reduced by employing best practices such as choosing cloud providers that support: (i) the use of standardised APIs wherever possible; (ii) wide range of programming languages, application runtimes and middleware; (iii) as well as ways to archive and deploy libraries of virtual machine images and preconfigured appliances. Overall, these findings suggest respondents do not currently have sufficient understanding on possible technical and non-technical issues of lock-in that can occur in the cloud environment. Thus, it is recommended that organisations remain meticulous when making decisions towards the selection of vendors, taking into consideration potential difficulties associated with switching vendors. However, it is probable for organisations to suffer financial loss if they did not make a strategically correct vendor selection decision from the very onset.

4.6.3 Well-informed Decision Making

The study has found that for UK organisations, when it comes to evaluating the business risks of vendor lock-in for or against cloud migration, surprisingly, a clear majority (66.4%) of respondents said making well-informed decisions before selecting vendors and/or signing the cloud service contract is an extremely important part of the decision-making process (refer to **Figure 4.14**). This signifies that as cloud computing becomes more widely used for various applications across different industry sector[s] and size[s], UK businesses are finding it extremely important to understand ways to maximize benefits and minimize the risks of lock-in. This is particularly important given the plethora of vendors in the market place today, with each offering businesses proprietary cloud-based services and contracts that have different specification (and legal agreements). Regarding the interpretation of this finding, our study suggests that the vetting process for selecting vendors is a critical aspect for effective cloud migration with minimized risk of lock-in. Moreover, such finding exemplifies the need for organisations to look beyond the vendor selection phase, and focus on constantly monitoring any development or changes in the cloud that may impact data security or hinder interoperability and

portability – thus facilitating a lock-in situation. However, the findings (in **Figure 4.14**) also reveal a gap in understanding, regarding how organisations should manage the risks of vendor lock-in. A sign of lack of understanding is explained by a smaller percentage (8.4%) of participants identifying the need to build perceived lock-in risks into initial risk assessment. This is quite enlightening, despite the relevance of this strategy in the vendor selection phase. Possible interpretation of these may be attributed to the general lack of understanding and experience (on the part of IT and business managers) in respect of technical aspects of complex distributed cloud-based solutions.

4.6.4 Contract Evaluation

One of the key observations from the research presented in this paper was that a substantial number of organisations in the survey did not negotiate their SLA and cloud service contract (refer to **Figure 4.18**). However, opportunities may exist for these organisations to choose providers whose contracts/SLA is negotiable. Furthermore, unlike traditional Internet services, standard contract clauses may deserve additional review because of the nature of cloud computing. In fact, for the UK businesses in the survey, regarding strategy to manage potential risks of lock-in at the contract level, 80.2% of respondents said contract termination (i.e. retention and destruction of data), quality of service (QoS) guarantee (66%), and data protection (including data and metadata ownership) agreements (62.3%) should be drafted in the cloud service contract. Perhaps, these terms should be included within the contract in plain and intelligible languages. In the light of such results, it should be underlined that the impact of lock-in effect could be instantiated by the provider using proprietary data formats and service interfaces. This renders interoperability and portability of data and services difficult. For this reason, it is recommended that businesses ensure whether and how cloud providers support data portability and interoperability – prior to signing the cloud service contract.

Concerns about contract lock-in have been a consistent theme expressed by survey respondents concerning the treatment of data on termination. Although, contractual issues of lock-in related to termination will typically depend on whether the contract comes to a natural and expected conclusion or terminated due to the breach of contract. In either case, as stipulated in (Leimbach et al. 2014), the contract should make provisions for termination and the consequent handling of data. There are three key issues for businesses to consider concerning data on termination: (1) data preservation following termination – in this case firms should ensure they have reasonable time to access data, (2) data transfer – put in place, adequate tools to support transferring data or applications to a new service or back in-house, considering presently there are no legal obligation requiring cloud providers to provide data export tools, and (3) data deletion following termination – also determine how corporate data has been deleted, including the deletion of metadata and caching, seeing as 18% of businesses surveyed identified the need for data protection and metadata ownership (see **Figure 4.20**). In addition to the subsequent strategies, a thorough risk assessment should also be adopted by

the enterprises to ensure that the benefits for moving on to cloud-based services outweigh the security threats and privacy risks. Security is considered a key requirement for cloud computing consolidation as a robust and feasible multipurpose solution (IDC, 2010). Likewise, in this study, businesses have identified security as a major barrier to cloud implementation. Key references such as cloud security alliance (CSA, 2009) highlight different security issues related to cloud computing. Evidence has shown that there may be issues involving enterprises meeting their legal obligation when their data is hosted outside of their local context (Bem and Huebner, 2007). Enterprises must take note of such issues in consuming cloud services. Issues related to data security and privacy risks should be appropriately addressed. Regulation is typically not the primary cause of these issues, though when compared to the perceived risks internal to some organisations operating environment. It can be safely deduced from these figures (see **Figure 4.7 & 4.8**) that many organisations in the study are cautious about the implications and conditions surrounding their accountability to legal obligations such as Data Protection Act (DPA, 2012). The DPA in the UK for instance, applies to personal data that is processed; processing is likely to include most of the operations that are likely to occur in the cloud, including storage of data (ICO, 2012). In this respect, employing an information asset management system will essentially provide the necessary level of controls to ensure sensitive information is protected and meets enterprise compliance agreement (Oracle, 2009).

The provision of cloud services very often requires processing of data in servers located outside one's jurisdiction. There should be more evaluations conducted to assess the true potential and apparent risks to protect enterprises (Aleem and Sprott, 2013). Cloud computing implementation is subject to local physical threats as well as external threats. As a further matter, UK organisations moving corporate data and placing them in cloud storage environment must consider the following three core information security objectives (Hogan et al. 2011): confidentiality, integrity, and availability. These are essentially relevant as they are deemed high-priority business concerns. Common solution for achieving confidentiality can be encryption using cryptography. In terms of integrity, considering most business models rely on IT for core functionalities and processes and, thus mission critical data integrity and availability must be ensured. Since moving data to the cloud incurs loss of control over redundancy, location, dependency on provider for support, and another relevant configuration. This leads to the need of sufficient SLA to address related security concerns and data privacy issues. This includes support for portability such that customer can act to change cloud service provider when needed to satisfy availability, confidentiality, and integrity.

4.6.5 Standards and Cloud-based Solutions

The impact caused by vendor lock-in problem due to lack of standards is what enterprises should be wary about when considering migration to cloud computing (Opara-Martins et al., 2014). Despite the number of studies in recent years underlining the high relevance of standards in cloud computing,

unfortunately this study reveals that most UK organisations still lack a comprehensive understanding on the importance of standards in minimising lock-in risks. In fact, as pointed out by (Leimbach et al. 2014), there are two ways a business can achieve the full potential of cloud computing (i) either by changing providers per their needs (ii) prioritising or simply combining different solutions to get the best of the breed services. However, this will require standards and interoperability to be supported by all providers, but it is often not the case. An informative example in this context is seen in research in (Govindarajan and Lakshmanan, 2010), arguing that many cloud providers are concerned with the loss of customer that may come with standardisation initiatives which may flatten profits, and do not regard the solution favourable. Based on our research findings, from a business perspective, we suggest the following as key measures to improve customer retention and engender trust in enterprise cloud migration: 1) the quality of service (QoS) guarantee, 2) data protection and metadata ownership, 3) contract termination, as well as 4) data export functionality. Furthermore, as discussed in authors' previous study (Sahandi et al. 2013), in the absence of standardisation, UK businesses willing to outsource and combine a range of services from different cloud providers to achieve maximum efficiency, irrefutably, will have trouble when trying to get their in-house systems to interact with the cloud. Likewise, the lack of standardisation also brings disadvantages, when migration, integration or exchange of computer resources is required. This is consistent with the research findings presented in this thesis (see **Figure 4.13**). Unsurprisingly these issues were identified from a business perspective, considering the important role of standards in at least mitigating such concerns. Hence, business stakeholders should be aware that decisions to adopt or move resources to the cloud require adequate risk analysis for potential lock-in. Based on this analysis and the evidence shown in **Figure 4.13**, author believes there are opportunities that exist for the regulatory and standard bodies to take the necessary action. One potential solution would be to standardise the APIs in such a way that businesses (or SaaS developers for example) could deploy services and data across multiple cloud providers. Thus, the failure of a single cloud provider/vendor would not take all copies of corporate data with it.

4.6.5.1 Standard Initiatives

Cloud-specific standards are regularly proposed to mitigate vendor lock-in and achieve portability and interoperability (Govindarajan and Lakshmanan, 2010). It is expressed in (Petcu, 2011) that many providers are concerned with customer churn rate that may come with standardisation. But according to (Lewis, 2013), unless there is a well-accepted and widely used standard, it remains a questionable solution. Therefore, as a partially adopted standard would represent a poor solution (Shan et al. 2012); many cloud vendors now support the creation and adoption of new standards by proposing them to standardisation groups. Clear examples of such cloud-specific standards are OASIS CAMP (2012) for PaaS and TOSCA (2012) for IaaS. Both specifications aim at enhancing the portability and

interoperability of applications across different clouds. We review the two OASIS cloud-specific standards (TOSCA and CAMP) and their potential for dealing with the lock-in problem.

- **TOSCA**

The Topology and Orchestration Specification for Cloud Applications (TOSCA, 2012), is an emerging standard that enhances service and application portability in a vendor-neutral ecosystem. TOSCA specification describes a meta-model for defining IT services. This metamodels defines both the structure of a service (topology model of a service) and its operational aspects (such as how to deploy, terminate, and manage this service). Service templates are interpreted by a TOSCA-compliant environment (e.g. OpenTOSCA, 2015), which operates the cloud services and manages their instances (TOSCA, 2012).

Managing cloud services requires extensive, mostly manual effort by the customers. Further, important cloud properties (such as self-service and rapid elasticity) can only be realised if service management is automated. In this aspect, TOSCA allows application developers and operators (DevOps) to model management best practices and reoccurring tasks explicitly into so-called plans (i.e. Workflows). TOSCA plans use existing workflow languages such as Business Process Model and Notation (BPMN) (Breitenbucher et al. 2014; BPMN, 2011), or the Business Process Execution Language (BPEL) (OASIS, 2007). To increase portability, TOSCA allows service creators to gather into plans those activities necessary to deploy, manage, and terminate the described cloud service. TOSCA also enables a cloud service creator to provide the same plan or implementation artefact in different languages (e.g. a plan can include the same functionality twice – in BPEL and BPMN). An application ported to the cloud using TOSCA can be composed of services provided by different cloud providers and a user can decide to a specific service with a similar one from a different vendor.

- **CAMP**

Cloud Application Management for Platforms (CAMP) is an Oasis cloud-specific standard designed to ease the management of applications across platforms offered as a service (PaaS) (OASIS, 2012). The CAMP standard defines a self-service management API that a PaaS offering presents to the consumer of the platform. The specified CAMP API provides a resource model to describe the main components of any platform offer. For instance, independent software vendors can exploit this interface to create tools and services that communicate with any CAMP-compliant cloud platform via the defined interfaces. Likewise, cloud vendors can also leverage these interfaces to develop new PaaS offerings, or adapt the existing ones, which would be compliant with independent tools. Thus, cloud users save time when deploying applications across multiple cloud platforms.

At present, the effort of deploying applications with vendor-specific tools across multiple PaaS cloud platforms is a non-trivial task. Developers and system operators often face the barrier of redeploying applications to other providers' platform because tools are incompatible. However, this can be simplified using the CAMP interface common to both source and target platforms. To simplify the deployment efforts and support migration across multiple cloud platforms, CAMP defines the Platform Deployment Package (PDP). A PDP is an archive containing a plan file together with application content files such as web archives, database schemas, scripts, source code, localization bundles, icons etc. This archive can be used to move an application and its components from platform to platform, or between a development environment and an operative target platform.

4.6.5.2 Portable Hybrid IT Environment

To infer from discussion in the preceding section, the vendor lock-in risk is a valid concern for organisations migrating to the cloud. Considering that lock-in is undesirable, and cannot be eradicated, then how can businesses mitigate its associated risks when migrating to the cloud? From a portability perspective, it becomes critical that organisations' data is sharable between providers, since without the ability to port data or application, it would become simply impossible to switch cloud service providers at all (Parameswaran and Chaddha, 2009; Cisco, 2010). Cloud portability is a salient consideration to enable organisations migrate a cloud-deployed asset to a different provider and it is a direct benefit of overcoming vendor lock-in (Mell and Grance, 2009). Generally, reconfiguration of systems and applications to achieve interoperability is time/resource consuming and may require a considerable amount of expertise, which could be challenging for some organisations. Therefore, from a business perspective, portability should be seen as a key aspect to consider when selecting cloud providers as it can both help mitigate lock-in risks, and deliver business benefits. This means allowing applications, systems and data components to continue to work correctly when moved between cloud providers' (hardware and/or software) environments (Lewis, 2013). Indeed, the need for organisations to easily switch cloud providers with their data alongside have been a consistent theme throughout the discussion presented hitherto.

To expatiate on the question stated above, it is helpful to view the situation from a business perspective after deploying a SaaS cloud service such as CRM (which per **Figure 4.10,** 52% of organisations have already adopted the cloud model). Suppose these organisations use the SaaS CRM and over time, perhaps, the terms of use or the price of the cloud-based CRM service become less attractive, compared to other SaaS providers or with the use of an in-house CRM solution. If the organisation decides to change providers for whatever reason, data portability aspects must be considered. For SaaS cloud services, data formats and contents are handled by the service provider thereby making data portability a major consideration. The issue of importance in a SaaS-level migration is the compatibility of the functional interface presented to end-users and any API made

available to other customer applications. To alleviate this problem, the APIs made available by the SaaS service should be interoperable with the interface provided by the on-premise application or data that is being replaced. On the other hand, the data handled by one vendor's software should be importable by the second vendor's software, which implies both applications must support the common format. Standard APIs for various application types will also be required. If the APIs are not interoperable, any customer application or data using the APIs will need to be changed as part of the migration process.

Data portability is usually of most concern in a SaaS, since in these services, the content, data schemas and storage format are under the control of the cloud service provider. The customer will need to understand how the data can be imported into the service and exported from the service. Further, SaaS applications also present interoperability barriers. The lack of adoption of standard APIs for SaaS applications makes switching from one SaaS application to another difficult as it involves a change in the interface. This also applies to any application or system belonging to the cloud service customers that use APIs offered by the SaaS application. Data synchronization is another concern, encountered in cloud interoperability and not in data portability (Petcu and Vasilakos, 2014). To further substantiate this argument, we elucidate on the need for a portable hybrid environment by highlighting two main categories of portability scenarios encountered in current cloud service market: 1) porting legacy applications or data; and 2) porting cloud native applications or data. In scenario 1, due to dependence on technologies and data organisation, the legacy software assets currently require a significant amount of effort to be invested in porting them into the cloud environment. Whereas in scenario 2, even when applications and data are written from scratch for a cloud environment, they are usually locked and targeted for a specific cloud (Petcu and Vasilakos, 2014). Thus, the effort of porting in a different cloud is usually a onetime exercise. However, in both scenarios, the main problem is that there must be a capability to retrieve customer data from the source cloud service and a capability to import customer data into the target cloud service. Thus, data portability is based on import and export functionality from cloud data services for data structures. This is commonly done through the existence of some API (or web interface) associated with the cloud service – it may be a generic API or a specific API, unique to the cloud service.

In light of such challenges, Buyya et al. (2010) claims that ensuring data portability is a major challenge for enterprises due to the large number of competing vendors for data storage and retrieval. The ability to move data also emerges as a management issue for cloud computing. Therefore, in response to the question of data movability, it is important to note that the API used for the source service may not be the same as the API used for the target service and that different tooling may be required in each case. The main aspects of data portability are the syntax and semantics of the transferred data. The syntax of the data should ideally be the same for the source service and the target service. However, if the syntax does not match (i.e., the source may use JSON syntax, but the target

may use XML), it may be possible to map the data using commonly available tools. If the semantics of the transferred data does not match between the source and target services, then data portability is likely to be more difficult or even impossible. However, this might be achieved by the source service supplying the data in exactly the format that is accepted by the target service. Therefore, on a long term, achieving data portability will depend on the standardization of import and export functionality of data and its adoption by the providers. The aim is to minimize the human efforts in re-design and re-deployment of application and data when moving from one cloud to another. To this end, it becomes vital that any enterprise cloud migration project can be carried out without any disruption to data availability since data is an organisation's most critical, ubiquitous, and essential business asset (Opara-Martins et al. 2014).

4.6.5.3 Potential of DevOps Tools for Avoiding Vendor Lock-in

Issues with cloud lock-in surpass those of technical incompatibility and data integration. Mitigating cloud lock-in risks cannot be guaranteed with a selection of individual open (technology-centric) solutions or vendors. Instead, the management and operation of cloud services to avoid lock-in should be addressed at a standardised technology-independent manner. In this respect, we present a concise discussion on the potential of DevOps (Humble and Farley, 2010), and of tools (such as Chef, Juju and Puppet) that support interoperable management.

DevOps is an emerging paradigm (Wettinger et al. 2014) to eliminate the split and barrier between developers and operations personnel. Automation underlies all the practices that constitute DevOps. The philosophy behind DevOps is to bring agile methodologies into IT infrastructure and service management (Humble and Farley, 2010). This is achieved by implementing the concept of "Infrastructure as Code" (IaC) using configuration management tooling. An automation platform is what provides the ability to describe an infrastructure as code. IaC automations are designed to be repeatable, making the system converge to a desired state starting from arbitrary states (Hummer et al. 2013; Nelson-Smith, 2011). In practice, this is often centred on the release management process (i.e., the managed delivery of code into production), as this can be a source of conflict between these two groups often due to different objectives (Nelson-Smith, 2011). DevOps approaches can be combined with cloud computing to enable on-demand provisioning of underlying resources (such as virtual servers, database, application middleware and storage) in a self-service manner. These resources can be configured and managed using DevOps tools and artifacts. As a result, end-to-end deployment automation is effectively enabled by using the DevOps approaches in cloud computing environments (Wettinger et al. 2014). Tools are emerging that address building out a consistent application or service model to reduce the proprietary lock-in risks stemming from customized scripting while improving deployment success due to more-predictable configurations. Today, several applications provisioning solution exists that enable developers and administrators to declaratively specify

deployment artefacts and dependencies to allow for repeatable and managed resource provisioning (OpenTOSCA, 2015). Below, we review some DevOps tools among the currently available ones that may help enterprises simplify their application release circle.

- **Chef**

Chef is a configuration management framework written in Ruby (Nelson-Smith, 2011). Chef uses an internal Domain Specific Language or DSL to express configurations. Configuration definitions (i.e. ruby-scripts) and supporting resources (e.g. installation files) in Chef are called recipes. These recipes are basically scripts written in DSL to express the target state of a system (Sabharwal and Wadhwa, 2014). Chef manages so called nodes. A node is an element of enterprise infrastructure, such as a server which can be physical, virtual, in the cloud, or even a container instance running a Chef client (Ruby, 2016). Chef provides APIs to manage resources on a machine in a declarative fashion. Chef recipes are typically declarative (resources which define a desired state) but can include imperative statements as well. Combining a Chef system together with cloud infrastructure automation framework makes it easy to deploy servers and applications to any physical, virtual, or cloud location. Using Chef, an organization can configure IT from the operating system up; applying system updates, modifying configuration files, restarting any necessary system services, applying and configuring middleware and applications.

- **Puppet**

Puppet is an open source configuration and management tool implemented in Ruby (Dutta et al. 2013) that allows expressing in a custom declarative language using a model-based approach (Puppet Labs, 2015). Puppet enables deploying infrastructure changes to multiple nodes simultaneously. It functions the same way as a deployment manager, but instead of deploying applications, it deploys infrastructure changes. Puppet employs a declarative model with explicit dependency management. One of the key features of Puppet is reusability. Modules can then be reused on different machines with different operating systems. Moreover, modules can be combined into configuration stacks.

- **Juju**

Juju is a cloud configuration, deployment and monitoring environment that deploy services across multiple cloud or physical servers and orchestrate those services (Ubuntu Juju, 2015). Activities within a service deployed by Juju are orchestrated by a Juju charm, which is a deployable service or application component (Wettinger et al. 2014).

In summary, as applications evolve to function in the cloud, organizations must reconsider how they develop, deploy, and manage them. While cloud computing is heavily used to provide the underlying resource, our review shows that DevOps tools and artefacts can be used to configure and

manage these resources. Thus, end-to-end deployment automation is efficiently enabled by employing DevOps approaches in cloud environments. But, cloud providers such as Amazon and cloud frameworks such as OpenStack provide cost-effective and fast ways to deploy and run applications. However, there is a large variety of deployment tools and techniques available (Gunther et al. 2010). They differ in various dimensions, most importantly in the metamodels behind the different approaches. Some use application stacks (e.g., AWS OpsWorks2 or Ubuntu Juju) or infrastructure, others use lists of scripts (e.g., Chef run) or even PaaS-centric application package descriptions such as Cloud Foundry manifests. This makes it challenging to combine different approaches and specially to orchestrate artefacts published by communities affiliated with the different tools, techniques, and providers. Nevertheless, these solutions are highly desirable because some communities share a lot of reusable artefacts such as portable scripts or container images as open-source software (Wettinger et al. 2013). Prominent examples are Chef Cookbooks, Puppet modules, Juju charms, or Docker images. Adopting a configuration management tool implies a significant investment in time and/or money (Delaet et al. 2010). Nevertheless, before making such an investment, an informed choice based on objective criteria is the best insurance that an enterprise has picked the right tool for its environment, as the focus is on deploying predefined application stacks across several (virtual or physical) machines.

4.6.6 Observations

This thesis confirms that UK organisations are increasingly adopting cloud services, and it also reveals that they have been progressively migrating services perceived as non-mission critical (i.e. where lock-in and security risks seem lower) such as general purpose applications suites, email and massaging applications. This strategy used allows the organisations to get a feel for how the cloud environment works before fully committing themselves. However, this is generally not the case for organisations surveyed. A lesser minority (see **Figure 4.10**) seem to have adopted core systems in the cloud (e.g. ERP and CRM), including accounting and finance applications. At present, as indicated by the Cloud Industry Forum (2014), cloud providers or vendors are better placed, if they ensure such capabilities like the trial or "test and see" strategy (whether completely free or paid for time limited pilot) is made available within their go-to-market strategy. It is worth underlining that, free of charge or low cost does not necessary mean free of lock-in risks or low proprietary lock-in risk. Organisations must be cautious of potential areas of lock-in traps and take adequate measures to mitigate their exposure; e.g. choice of operating environment, programming models, API stack, data portability etc. Further, businesses should take heed of other legal, regulatory, or reputational risks that may exist. This is vitally important if the data involved is not just for testing, but constitutes real corporate data, perhaps even confidential or personal data. It is interesting to note that 28% of organisations surveyed have already adopted the cloud model for hosting accounting and finance applications (refer to **Figure 4.10**).

4.7 Chapter Summary

On a conclusive note, it is believed that the discussions presented herein, above all, indicate hypothetically that vendor lock-in risks will reduce cloud migration, which in turn affects the widespread adoption of cloud computing across organisations (small or large). Thus, an emerging research agenda arises as to investigate: 1) ways to come up with multijurisdictional laws to support interoperability and portability of data across cloud providers' platform, along with effective data privacy and security policies; and 2) novel ideas of avoiding vendor dependency on the infrastructure layer, platform, and through to the application layer as lock- cannot be eliminated, but can be mitigated. However, these require, not just tools and processes, but also strategic approaches – attitude, confidence, comfort, and enhanced knowledge of how complex distributed cloud-based services work. Sometimes the inhibitor to cloud adoption and migration in most organisations, in principle, are the attitude, knowledge, and confidence of the paramount decision makers. Thus, for most organisations today, the challenge is clear that they simply do not understand potential effect of lock-in to the business. While the business benefits of cloud computing are compelling, organisations must realise that achieving these benefits are consistent with ensuring the risks of vendor lock-in and security implication of such risk is clearly understood upfront. When identified, such risks should be mitigated with appropriate business continuity plans or vendor selection, prior to migration to the cloud. Based on the review of relevant literatures (in the preceding chapters) and the empirical data analysis performed in this chapter, the subsequent chapters of this thesis presents the proposed framework to avoid vendor lock-in risks in cloud SaaS migration. This is followed by an evaluation and validation of the proposed decision framework based on IT practitioners, academia, cloud specialists and expert views.

Chapter Five

5. Proposed Cloud Migration Decision Framework

5.1 Introduction

Now, with respect to the outlined objectives (i.e. O.5) of this PhD thesis given in Section 1.3, this section introduces the proposed decision framework, designed for use by enterprises that are already consuming or considering adopting cloud-based SaaS offerings. The decision framework can be used by such organisations for reviewing their business needs and weighing up the potential benefits and opportunities against the risks of vendor lock-in, so that the transition from source to target cloud computing environment is strategically planned and understood. For the development of the proposed decision framework, please refer to our previous for a comprehensive discussion. This work was initially targeted at the vendor lock-in challenges of cloud SaaS services adoption and migration. Author has examined the requirements of cloud software (SaaS) application migration from four distinct viewpoints; user view, functional view, implementation view and deployment view.

The user view focuses on the cloud SaaS system context, the parties, roles, sub-roles and cloud computing activities involved. The functional view covers functions necessary for the support of cloud SaaS computing activities. However, the implementation view comprises the functions necessary for the implementation of a cloud SaaS service within service parts and/or infrastructure parts. While the deployment view is concerned with how the functions of a cloud SaaS services are technically implemented within already existing infrastructure elements or within new elements to be introduced in this infrastructure. Note, while details of the user and functional view are comprehensively addressed within this paper, the implementation and deployment view are related to technology and vendor-specific cloud computing SaaS implementations and actual deployments (i.e. migration), and are therefore out scope in this paper.

5.2 Framework Design Process

During the framework design process, cloud computing researchers and ICT practitioners together with enterprise decision makers participated and contributed to the design and development of the decision framework for avoiding cloud vendor lock-in risks. Once the decision framework was developed, it was validated by practitioners from many organisations that are already using cloud SaaS services for at least one application domain. These included organisations that also utilise a combination of cloud services and internally owned (on-premise) applications (i.e. so-called hybrid IT estates). During the validation process, all feedbacks and suggestions offered were incorporated into the subsequent version of the framework.

Our proposed decision framework is broken down into discrete manageable steps (as shown in **Figure 5.1**) that support the move from one cloud SaaS solution to another from the same or a different provider (e.g. moving from one cloud customer relationship management (CRM) solution to another). The decision framework outlines series of activities that are required to make informed decision to avoid vendor lock-in before switching to or from one cloud SaaS provider(s) to another. This ensures appropriate pre-planning and due diligence so that the correct cloud service provider(s) with the most acceptable risks to vendor lock-in is chosen, and that the impact on the business is properly understood (upfront), managed (iteratively), and controlled (periodically).

A core function of the decision framework is to act as an assessment tool for key stakeholders when selecting cloud services, and a framework to guide decision makers who are interested in avoiding lock-in when they choose to use a cloud SaaS service. Thus, the resulting framework can be applied to either the migration (or on-boarding) and the on-going management and integration of cloud SaaS services with available ICT facilities in-house. **Figure 5.1** summarises the vision of this framework. Note, two unique underlying concepts of the framework are the decisions that need to be made, and the tasks (or activities) that need to be performed to support these decisions – which in turn affects their outcome (i.e. artefacts). The decisions are the key part of the framework consisting of six concrete steps (i.e. decision steps) as explained later in subsequent sections. Tasks (or activities) which need to be performed in the framework to support these individual decisions, may also affect other decision steps. In other words, each decision step (e.g. step 1) has a direct or indirect impact on the others. Thus, all the decisions and tasks required as well as their relationships and influences constitute a model which offers guidelines to support stakeholders in the decision-making process to avoid vendor lock-in risks in cloud SaaS migration. Furthermore, across the six main decision steps (in Figure **1**), the underpinning decision the proposed framework supports refers to is: "How to select a cloud service provider and its offerings that fits the organisations needs in terms of contractual agreement, cost, and expected performance based on compatibility, interoperability, portability and standards, compliance requirements and security concerns?".

5.3 Phases of the Proposed Decision Framework

This section summarises the series of migration steps into a standardised practical approach for successfully managing cloud SaaS application migration to avoid vendor lock-in risks. For this approach, we assume that the business case for migration has been established and a consensus has been reached to begin the SaaS migration process from one cloud SaaS vendor to another (or back to internal IT service provision). However, for instance, if the cloud consumer only attempts to use the potential SaaS offering on a trial basis, agreement and understanding between both parties (i.e. provider and consumer) should be reached first, prior to using the service. Only when such agreements are established should the consumer provide the cloud service provider with user

credentials to authenticate the user and grant access to the trial cloud SaaS service – which can be tested by the cloud service consumer for business purposes.

The decision process for cloud SaaS service migration to avoid vendor lock-in risks, illustrated in **Figure 5.2**, progresses through three distinct phases (1, 2, 3) – selection, provision, and management; that are further divided into six discrete manageable steps as further explained in the subsequent section. These six decision steps are centred on the guided identification and analysis of main risk factors that either influence or intensify a cloud lock-in situation. Our six-step decision framework for cloud SaaS migration is aimed at supporting organisations in making informed cloud service selection and migration decisions to avoid vendor lock-in.

Note, the six steps and corresponding activities should be carried out per the process workflow shown later in **Figure 5.6.** The basic premise is that an enterprise only commits resources one step at a time, so as each step is completed, there is the option to stop without losing the initial investment. This incremental approach reduces the risk associated with cloud projects. The three main phases of the cloud SaaS migration process are:

- Phase 1: *Service Selection and Evaluation*
- Phase 2: *Contract and Service Provision*
- Phase 3: *Service Validation and Management*

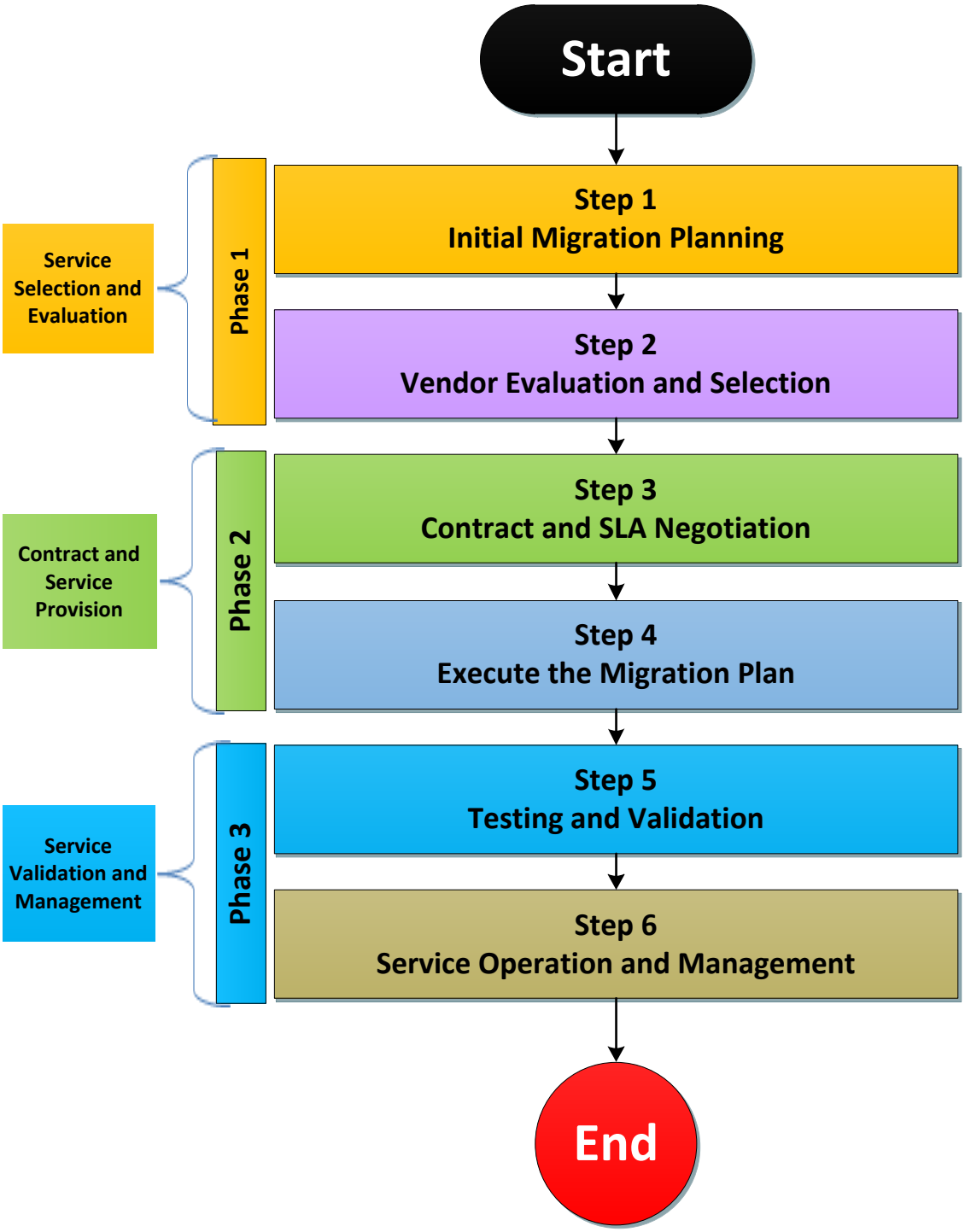


Figure 5.1- Overview of the Proposed Cloud Migration Decision Framework

Figure 5.2- A Lifecycle for Managing Vendor Lock-in Risks in Cloud SaaS Migration

5.3.1 Phase 1: Service Selection and Evaluation Process

Phase 1 mainly involves strategies for conducting effective business and IT requirement analysis to meet enterprise needs. These include efficient pricing, contracting, and security parameters, as well as procedures to engage cloud service providers in enabling portable and inter-operable cloud solutions. The activities performed in Phase 1 involves but are not limited to the following; examining the cloud service offerings of (one or more) SaaS service providers to determine if the service offered meets the documentation of each service. This can include technical information about the service, and its service level agreement (SLA), plus business information including pricing, as well as negotiating terms for the service (i.e. only if the service provider permits variable terms for the services). The output of Phase 1 is a detailed migration plan and road-maps for cloud deployment,

service provider selection, and contract negotiation. These road-maps outlines series of activities required to move a SaaS application, and prioritize on-premise services that have high expected value and high readiness to maximise benefits received and minimize delivery risks of vendor lock-in. The service selection and evaluation phase starts by analysing first the current situation (i.e. stakeholder analysis, business and IT inventory etc.) within an organisation, and identifies potential risks, constraints and opportunities for cloud SaaS migration planning. Being the initial phase of the SaaS migration process, the objective is to clearly understand and identify which IT services are appropriate for SaaS replacement or cloudification (i.e., how to use and access the legacy applications as services in the cloud), determine cloud readiness and technology lifecycle, decision making regarding which cloud provider to choose, contract with and/or negotiate SLAs. Defining exactly which SaaS cloud service an organisation intends to provide or consume is a fundamental initiation phase activity in developing an enterprise cloud roadmap. The decision-making process in this phase is an important aspect during the vendor selection and evaluation step. Reason being that, the vast diversity among available cloud SaaS offerings makes it difficult for the enterprise to decide whose vendor services to use or even to determine a valid basis for their selection. The decision steps and supporting activities involved in this phase are shown in **Figure 5.3**.

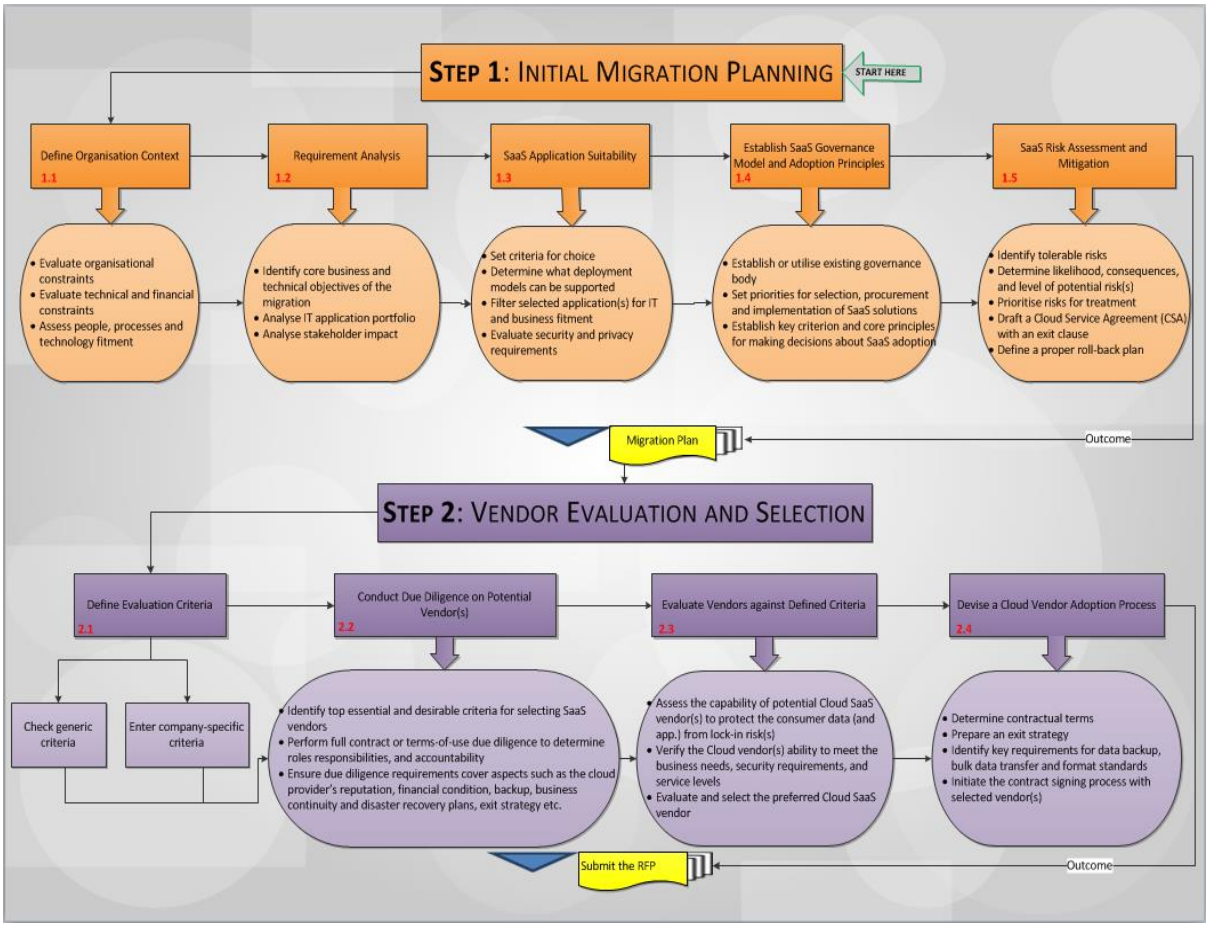


Figure 5.3- Key Activities and Outputs for Phase 1

5.3.2 Phase 2: Contract and Service Provision Process

The contract and the service provision process involve accepting the contract for the cloud service and performing the registration with chosen cloud SaaS service provider. This registration process may involve activities/tasks such as the provision of user credentials to enable cloud service provider to authenticate the user and grant access to the cloud SaaS service, as well as the invocation of the cloud service which then operates and delivers its specified outcomes. In phase 2 thereof (**see Figure 5.4**), the actual migration of data and the application component (i.e. business logic) are carried out, tested and evaluated to validate the migrated SaaS service performs as expected, and in accordance to the signed contract(s) by both parties. In terms of mitigating vendor lock-in risks, to be successful in this phase 2, organisations must think carefully through many of factors including interoperability and portability, security, strategies to contract effectively and realize value, and capability to integrate services (i.e. connect ICT systems to cloud services). Note, the capability to connect ICT systems to cloud services in this case includes integration between existing ICT systems and cloud services which involves the connection of existing ICT component(s) and applications with target cloud SaaS services and connection of customers (on-premise) monitoring and management systems with the cloud providers monitoring and control of services. Processes such as data loading and extraction, technical testing (functional and non-functional, integration, interoperability, portability, performance, security) compliance, and audit are implemented and tested for user acceptance in this phase.

Generally, phase 2 requires effective approaches and trade-off analysis for moving data and/or application components from one SaaS cloud provider to another. More significantly, this phase 2 helps to identify, evaluate, and address the impact of the cloud ecosystem during any change caused by future technology services which may be introduced, modified, or eliminated within the overall enterprise architecture. To be successful in the cloud service provisioning phase 2, organisations must think carefully through a number of factors including accessing the impact of cloud services on existing processes, systems and services, mapping of business data between cloud service customers using existing ICT systems and cloud services, invoking cloud service operations from existing ICT components and applications, with the supply of input data and the handling of output data, provisioning of access rights for cloud service users. Additionally, this extends to also involve defining and implementing security related requirements, including the confidentiality and integrity of data flows.

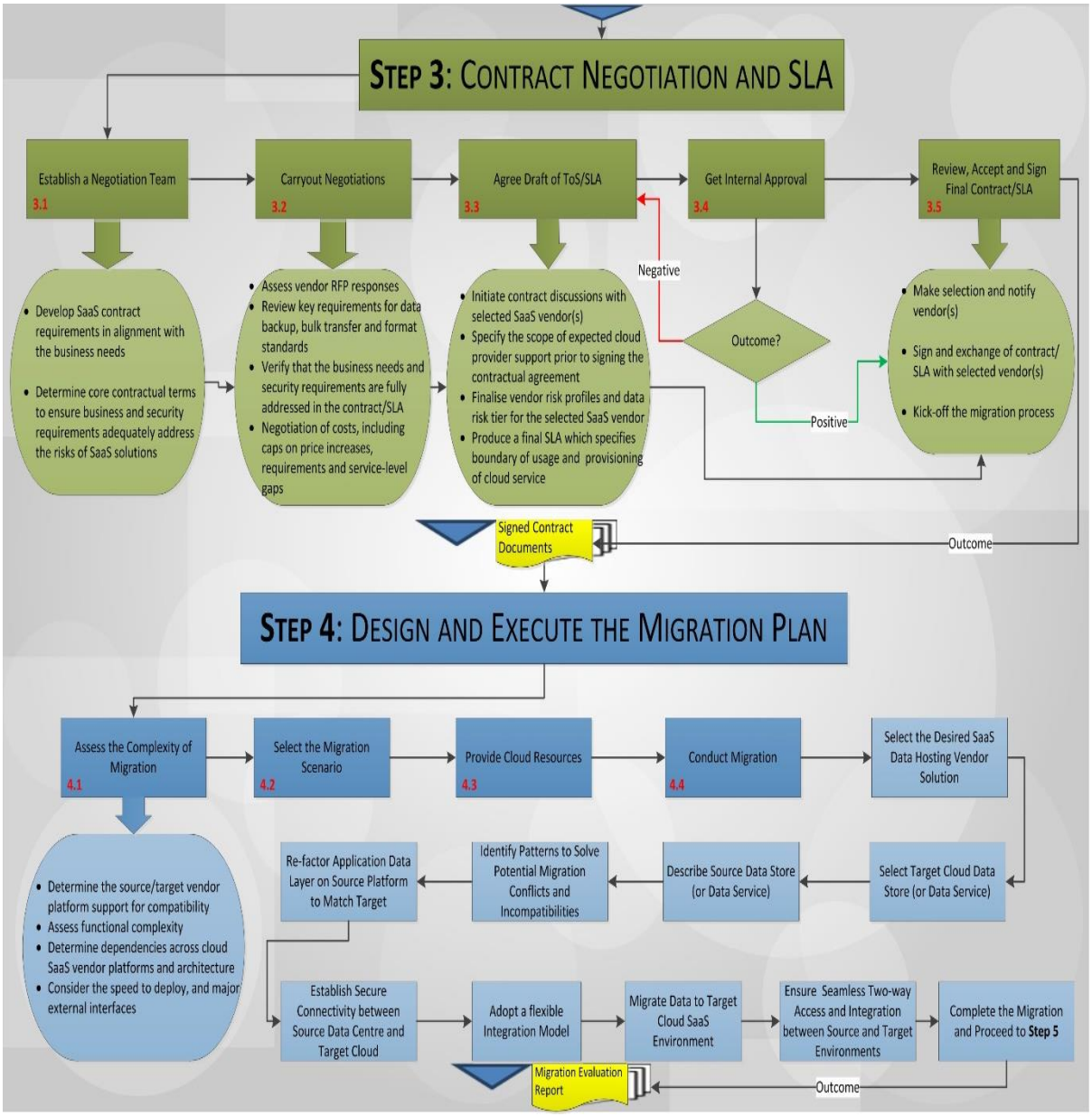


Figure 5.4- Contract and Service Provision Phase 2

5.3.3 Phase 3: Service Validation and Management Process

The service management (phase 3) focuses on activities such as monitoring the behaviour of the ICT environment of the target cloud SaaS provider infrastructure to ensure that the migrated (data and/or application components) service(s) are meeting the service level objectives and terms of the SLA. Thus, the activity in this phase extends to monitoring the metrics for each service and comparing them with the service targets required by the SLA for the service. In this case, the consumer can take actions when the metrics do not meet the values required by the SLA, as well as report problem if compliance cannot be maintained.

Essentially, phase 3 (see **Figure 5.5**) is required to maintain, monitor, optimise and manage the migrated SaaS service. The output of this phase defines compliance agreements, metrics to ensure required QoS is maintained and monitored, and effective attributes to engage service providers in discontinuing or terminating contracted cloud SaaS services when required with minimum or no lock-in effect. To be successful in phase 3, enterprises must view cloud computing with a new way of thinking that reflects a service-based focus rather than an asset-based focus. Some of the few considerations to consider in this phase include a shift in mind-set, implement application in accordance with SLA, actively monitor and re-evaluate periodically, log application in operational state, identify rollback (to internal IT-service provisioning) requirements or infrastructure consolidation opportunities.

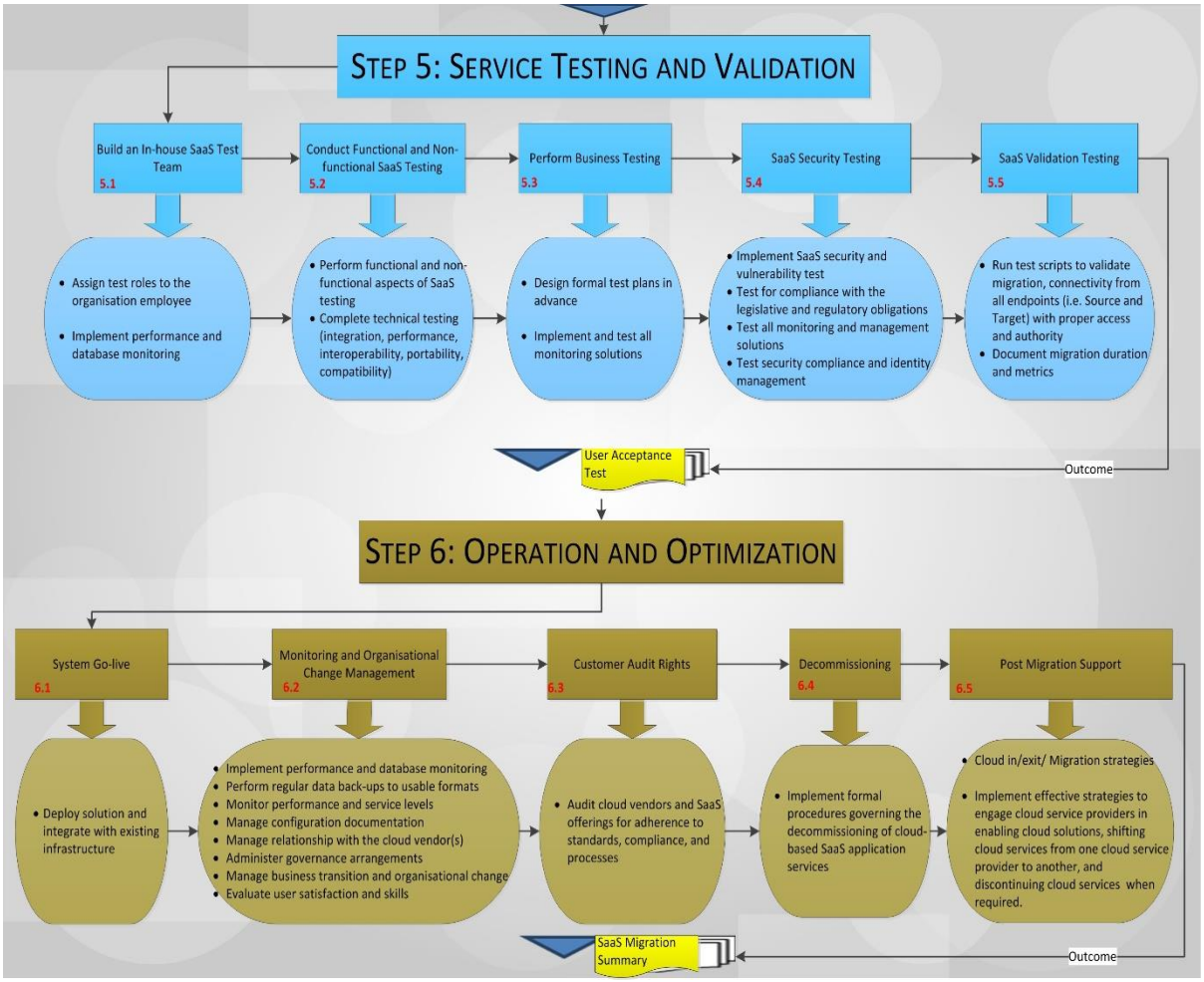


Figure 5.5- Service Validation and Management Phase 3

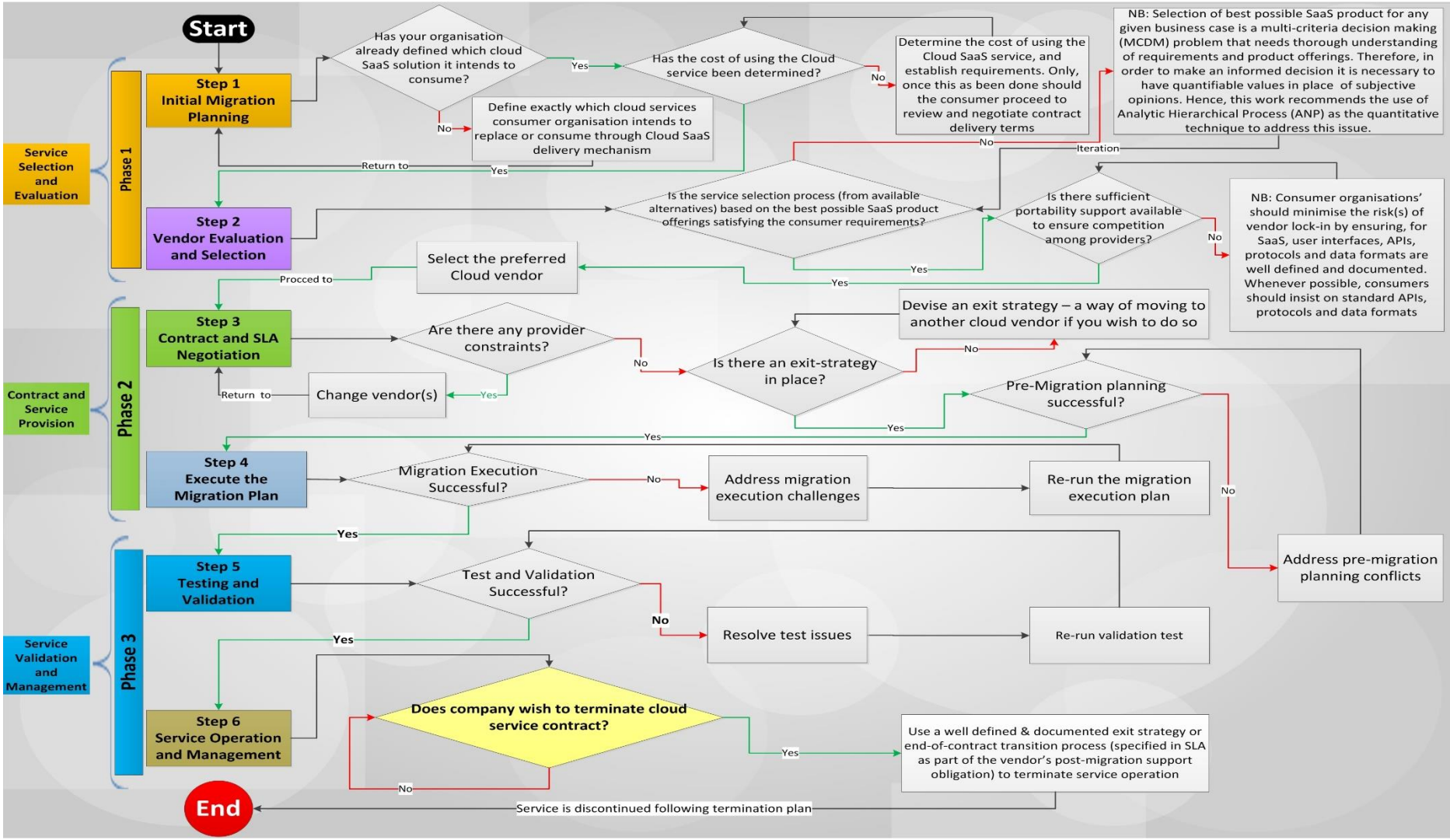


Figure 5.6- Process Workflow for the Proposed Cloud Migration Decision Framework

5.4 Sequence of the Proposed Cloud Migration Decision Framework

In subsequent section, we elaborate on the six main decision steps in our proposed framework for avoiding vendor lock-in risks in cloud SaaS migration. Each step provides a prescriptive series of tasks, supporting activities and decisions that cloud service consumers should consider when switching between SaaS vendors for a cloud service, or migrating existing applications to cloud computing to ensure workload portability, interoperability, compliance and security requirements are met.

5.4.1 Step 1 – Initial Migration Planning

The first process is the migration planning step where preliminary migration tasks such as migration requirements analysis, cloud services to use, as well as a feasibility study to identify or determine whether the migration is financially, technically, and legally feasible or not. This decision step is organised into five main sub-processes and eighteen supporting activities, which should be carried out per the sequence in the lifecycle diagram (refer to **Figure 5.2**). Note a cloud broker can be consulted prior to this step to create pre-agreements with cloud service providers. The broker can enable cloud SaaS service customers to select cloud SaaS service providers from a service catalogue (or marketplace) possibly negotiating service details (e.g. service level objectives) at selection time. In this case, however, the cloud service broker only acts during the contracting phase of the service, between the cloud SaaS service customer and cloud SaaS service provider.

In step 1, a detailed assessment of the existing business and IT environments is conducted to understand the applications appropriate for moving to the cloud or replacing with a SaaS alternative *(i.e. **Step 1.1 – Design organisational context**)*. Being the starting point for each migration project, enterprises should use this step to analyse if what they want to achieve by migrating to (or adapting systems and applications for increasingly heterogeneous cloud data centre architectures) is feasible to them in terms of technology, processes and business *(i.e. **Step 1.2 – Perform requirement analysis**)*. To decide which application layer(s) are possible for the cloud migration and/or replacement implicates measures of enterprise compliance in terms of internal and legal regulations. Moreover, classified data on the application data layer might obstruct seamless migration approaches; also application logic on the business layer can possibly expose problems in case it contains enterprise processes that constitute competitor advantage. In this sense, security concerns can be raised regarding critical data and communications. For example, such concerns are especially related to data communication occurring between application layers in case of a hybrid cloud migration approach. Data security concerns in term of data privacy regarding the data layer have to be considered. In this case, approaches like confidentiality cloud data patterns explored in works of () aid to overcome concerns like these.

However, since a simple replacement of application layers with a cloud computing service is not applicable in most cases without at least entailing application adjustment. Hence, instead of only gathering business and technical requirements, enterprises should also collect information pertaining to project management (i.e. who will manage the project, and how), the potential cost of the migration, migration approaches, tools to use, stakeholder impact analysis and so on. Additionally, a detailed inventory of the application portfolio is also created to assess the impact of application migration on the cloud ecosystem, including other applications, integration with other services, reporting, and backup and recovery processes *(i.e.* ***Step 1.3 – SaaS application suitability****)*. The business and IT portfolio analysis and the consecutive security analysis with other critical cloud system requirements such as interoperability, portability, auditability and compliance are the basis for all decisions and concepts *(i.e.* ***Step 1.4 – Establish SaaS governance model****)*. If the resulting estimations fulfil the organisation's expectations and needs, the migration planning will proceed (pending the outcome of established governance model in place) even though the company may encounter other challenges derived from the cloud provider architecture and constraints in subsequent steps. It should be noted that any mistakes or uncertainties during this step can affect the whole migration and operation because the pre-requisite for all following steps and accompanying decisions (and tasks) are defined during the planning phase. Amongst these activities, a major decision task required in this initial migration planning step is the evaluation of the risk and mitigation options available to the enterprise migrating to or changing the cloud SaaS vendor. This analysis will dictate if the migration planning can proceed or not dependent on how the company rates the risk of lock-in. The idea is to anticipate the detection of potential lock-in risks, migration conflicts, and organisational constraints, which might affect the SaaS migration decision prior to any further analysis of application itself, or of the candidate cloud service vendors. A decision tree illustrating the process workflow of this task *(i.e.* ***Step 1.5****)* is shown in **Figure 5.7**. The output artefact of all the activities and tasks performed in Step 1 is a migration plan. Most importantly, the migration plan essentially captures information regarding the consumer's business environment, technical architecture or legal characteristics that is considered relevant to the migration and/or implementation of the SaaS cloud service. Some examples of such characteristics are policies, guidelines, laws and any other rule or standard that the organisation must abide to and which may influence its adoption of cloud-based solutions. Below are some important questions usually raised to guide the initial migration planning step:

- Does the vendor's SaaS software solution support open data formats that are not owned by any individual company, but are instead owned and supported by a community?
- Is it written in the SaaS contract agreement that the consumer owns its data?
- What will be the cost of leaving or switching SaaS vendors?

- Does the SaaS vendor offer resilience, business continuity and disaster recovery support that is required?
- How is the SaaS application itself protected, and how is that protection maintained over time?
- Can users easily get their data out of the vendor's SaaS solution? Etc.

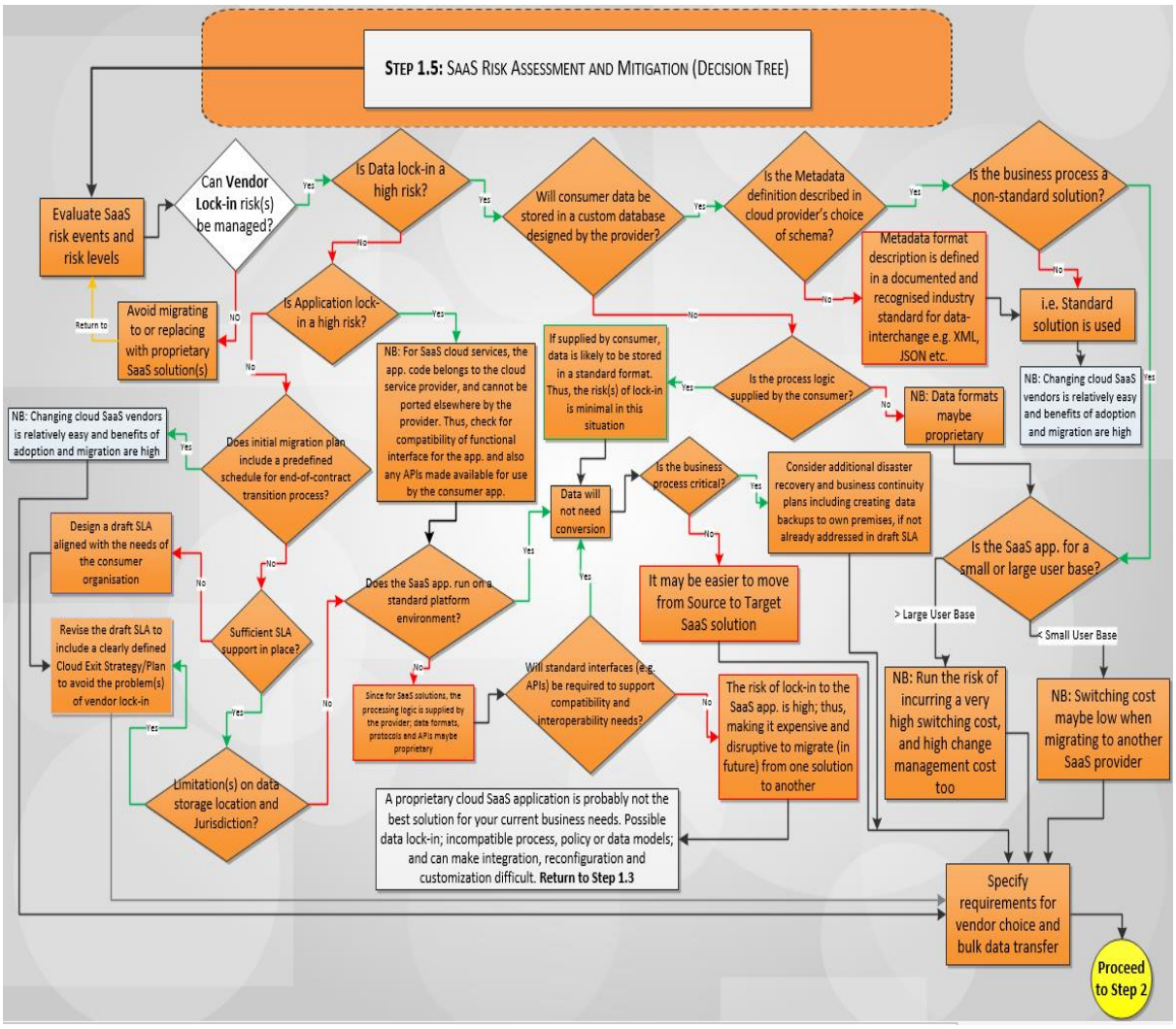


Figure 5.7- Decision tree illustrating the process workflow for Step 1.5

5.4.2 Step 2 – Vendor Evaluation and Selection

With so much of a company's asset invested in IT, and increasing reliance on outsourcing of many complex enterprise IT systems (i.e. services and products) to cloud-based SaaS environment, the job of a consumer is not only important but also challenging. Deciding on which cloud SaaS vendor and/or its service offering to be used depends fundamentally on the type of cloud solution that is appropriate for the enterprise *(i.e. **Step 2.1 – Define evaluation criteria**)*. Cloud SaaS consumers must define and measure what "best value" means for them, and execute procurement decisions accordingly. To identify best value, the buyer must interface with technical, legal, and operations

experts within the consumer's company, and act as an expert negotiator and coordinator across many internal and external parties (Beil, 2010) – *i.e.* ***Step 2.2 – Conduct due diligence***. Aspects like costs and functional suitability are some of the most important criteria in enterprise selection of a cloud provider and its offering, but an evaluation will likely and should involve the vendors' general reputation. To address this issue, consider several characteristics or attributes like reference projects, benchmarks, reports, etc. regarding a vendor's reputation and also like resources, knowledge, skills etc. in terms of the vendor's capabilities. Based on this data gathered for various candidate cloud vendors, a proper vendor evaluation can be performed to identify an appropriate vendor in terms of social or soft facts beside those technical and organisation requirements defined in Step 2.1

At a glance, vendor evaluation and selection is the process by which the consumer (i.e. buyer) identifies, evaluates, and contracts with cloud service vendors. There is also a growing audience for cloud vendor management research, as the importance of fostering talent by employing buyers with analytical expertise, general management backgrounds, and deep knowledge if a purchasing category becomes widespread (Reinecke et al. 2007). A key element in the vendor evaluation and selection step is the Service Level Agreement (SLA) that spells out the agreed service levels for important metrics such as contract termination (i.e. retention and destruction of data), quality of service (QoS) guarantee, security and data protection (including data and metadata ownership), business continuity, and disaster planning. Depending on the legal situation in the country of the cloud customer, the contracts should be negotiated and regularly adopted if necessary to make the terms more balanced and appropriate to address own circumstances and meet their heightened business requirements *(i.e.* ***Step 2.3 – Evaluate vendors based on specified criteria****)*. For this and many other reasons (Opara-Martins et al. 2016), it is recommended that during the decision-making process regarding which provider to choose, enterprises must ensure whether and how cloud providers support data portability, interoperability, and compliance to specific legal frameworks – prior to signing the cloud service contract *(i.e.* ***Step 2.4****)*. The key activity performed during the vendor selection and evaluation step is to devise a cloud vendor adoption process as illustrated in **Figure 5.8**. The overall output artefact of step 2 is a creation of a SaaS request for information (RFI) and the subsequent request for offer (RFO) documents. Some of the important questions that are usually raised in this step are:

- Is the cloud vendor based on open technology (e.g. cloud foundry, open stack) facilitating greater portability with other providers?
- Is the cloud SaaS vendor responsible for ensuring that the provided service is compliant to relevant regulations and that subcontractors are also compliant?
- How hard will it be to change the SaaS solution for another one from a different vendor? What kind of support is offered, how and what is it charged? How does the vendor meet the unique security requirements of your industry?

- Will the SaaS solution enable organisations to effectively manage operational, security and compliance risks? Does the SaaS product conform to relevant industry standards?
- Will the SaaS vendor allow users to export data/configurations/code to target architecture of choice without relying on proprietary libraries/services?

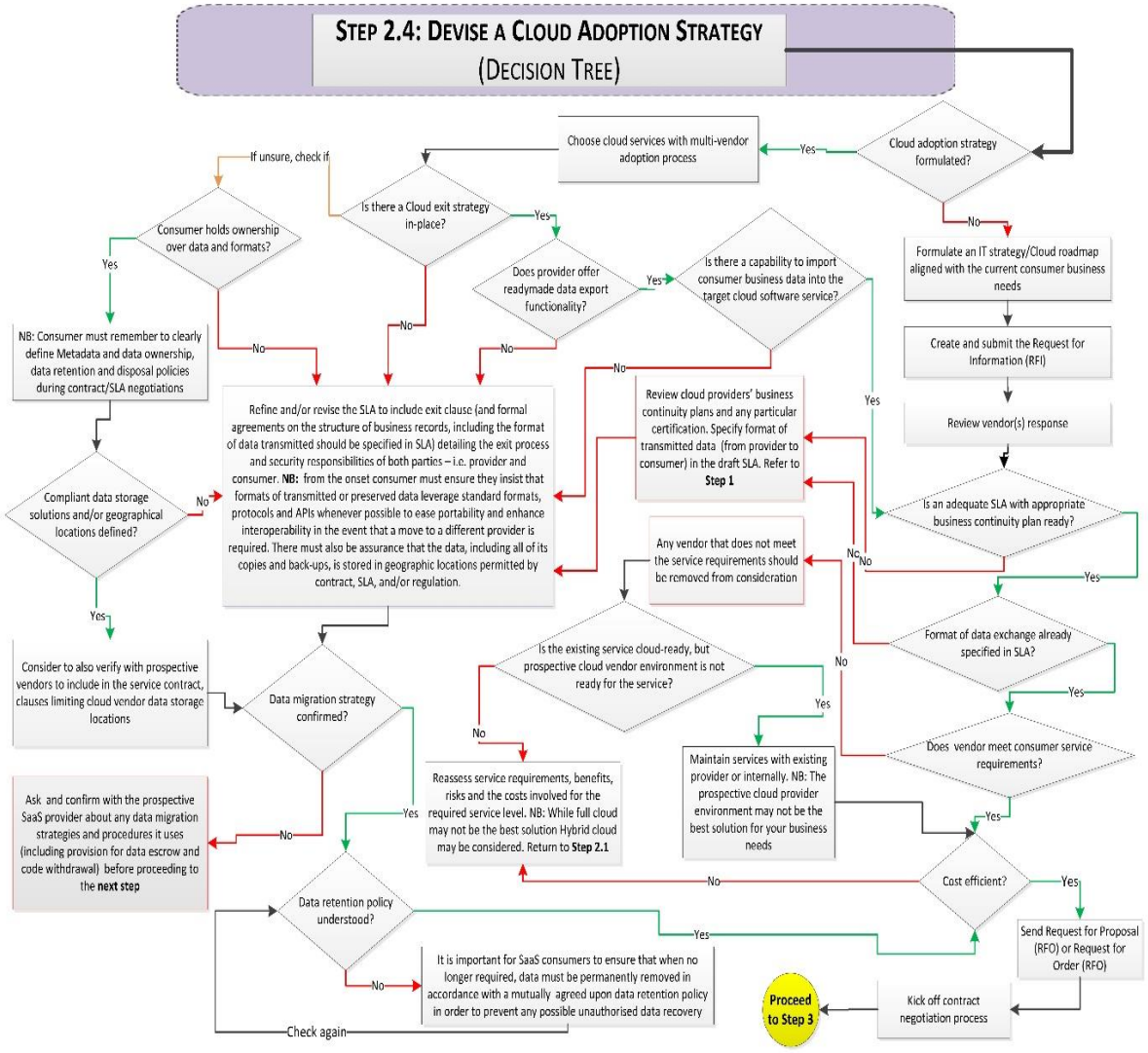


Figure 5.8- Decision Tree for Devising a Cloud Adoption Strategy (Step 2.4)

5.4.3 Step 3 – Contract and SLA Negotiation

This decision step involves activities that focus on defining and agreeing on selected service level metrics and management. The common tasks include defining how the metrics are reported and managed, ensuring that SLA targets are met. Cloud computing providers can create lock-in through contractual terms, or through the physical holding of customer's data. In this regard, there is an economic benefit to the vendor in the form of a regular revenue stream, but not so much of business benefits to consumers. From a commercial perspective, this puts the vendor in the position of strength when it comes to renegotiate the commercial terms of agreement. For this reason, it is important not

only to review the contract before signing but also negotiate the Service Level Agreement (SLA) around crucial elements like data ownership and termination conditions protecting against risks of vendor lock-in. Once the costs of using the services established and requirements have been determined, the consumer proceeds to review the contract and delivery terms, negotiate to try to reduce price or improve performance, and select their preferred service. But, before doing these, the question of exit strategy should be considered (see **Figure 5.9** for example – *i.e.* ***Step 3.5***). When negotiating with a new vendor, or re-negotiating with an existing one, you should be sure that you have an exit strategy. Such strategy should consider all the issues that were raised in the preceding steps to minimise not only the initial migration cost but also the cost of managing, operating and discontinuing the SaaS application after it has been deployed in the cloud environment. The cloud customer should also consider the contract terms and the cost of making the change. Insisting on requirements for supplier's choice and bulk data transfer will help users achieve this. From a business perspective, there is more than one way to get locked-in to a cloud vendors system; an often-overlooked method is through a contract.

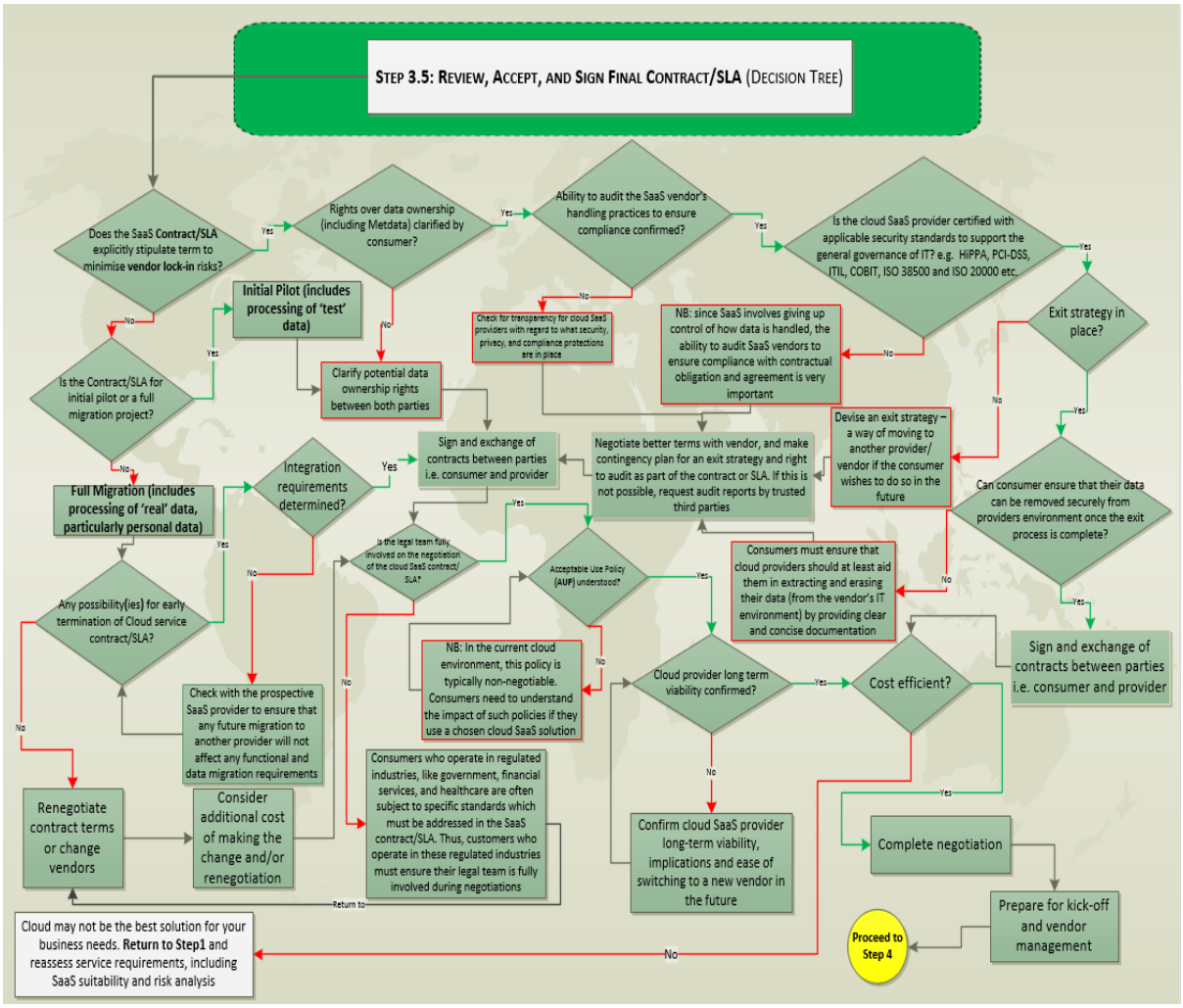


Figure 5.9- Decision Tree for Reviewing and Signing Cloud SaaS Contracts (Step 3.5)

5.4.4 Step 4 – Design and Execute the Migration Plan

Once an application or a set of applications is identified as a potential candidate to migrate onto a virtualized target cloud SaaS environment, the next important step is to categorize the application as simple, medium, complex, or very complex depending the various parameters of application hardware and software study. Thus, complexity categorization *(i.e. **Step 4.1**)* from an application perspective is equally important in understanding the migration. The work of (Banerjee, 2012b) indicates the complexity range for applications from simple to very complex. Based on the classification of application types (in Step 1), one can decide which strategy (e.g. Forklift or Hybrid migration) to apply for what type of application *(i.e. **Step 4.2**)*. Nonetheless, in the subsequent step *(i.e. **Step 4.3**)*, the actual migration tasks such as data extraction, data loading, integrating services, application architecture adaptation, definition of the security concept for migration and operation phase, rollback scenarios are executed. These include defining the specification of functional and non-functional requirements with respect to the SaaS target data store (or data service), which is also required in this step to define when the source SaaS data store (or data service) to identify and solve potential migration conflicts. Conflicts are identified by checking the compatibility of the properties of the target data and the store selected. To address these conflicts, special focus should be given to adaptation of the data access layer and the business logic layer of the migrated SaaS application. For instance, when considering databases (whether logically locate at the data layer, or more precisely at the database layer) it is important to understand that even if the cloud service provider offer databases commonly used on-premise, like Oracle databases, SQL server, and MySQL. There may also be occurrences of incompatibilities based on different database versions or characteristics and functionalities which are not implemented by the service provider. Hence, when choosing the appropriate storage option, it is crucial to understand one size does not fit all. However, there are several dimensions that one might have to consider so that the application can scale to their business needs appropriately with minimal effort. One have to make the right tradeoffs among the various dimensions identified in (Varia, 2010), namely - cost, durability, query-ability, availability, latency, performance (response time), relational (SQL joins), size of object stored (large, small), accessibility, read heavy vs. write heavy, update frequency, cache-ability, consistency (strict, eventual) and transience (short-lived). Weigh your trade-offs carefully, and decide which ones are right for your application.

Therefore, the actual migration plan *(i.e. **Step 4.4**)* should be executed once the cloud service consumer has decided that there are no critical migration conflicts making it impracticable for the SaaS application migration within the cloud (see **Figure 5.10**). However, as pointed out by (Bassera et al. 2012), given the emerging nature and relative immaturity of current cloud technology offerings, thus it is recommended that the organisation proceeds with a pilot migration project, prior to implementing the actual migration. This will help to investigate if the behaviour of the SaaS cloud

application in the cloud will function as expected. In this respect, it is highly advisable to consider multiple migration scenarios, possibly involving different migration strategies and costs. Moreover, during the migration phase, a rollback to the beginning must be possible. Although the cloud data store might be fully compatible with the data previously used as the migration requires at least a change in the database connection string in the data access layer. This means that the level of data access is important to be addressed appropriately due to its responsibility of ensuring appropriate data access functionality. To address this importance, Strauch et al. (2013) and Andrikopoulos et al. (2013) developed several cloud data patterns concerning functional, non-functional, and confidential challenges and Hajjat et al. developed an algorithm in (2010) to ensure data access after migration to the cloud. Thus, the impact of SaaS data migration in the cloud depends on aspects like the incompatibilities of the source and target data store. Therefore, in this step, migrating the data components of a SaaS application should entail the configuration of the connections to the sources and target data stores or services by requiring user input such as location parameters, credentials etc. This step also requires adapters for the corresponding source and target stores, bridging possible incompatibilities between them, and/or reuse of the data export and import tools offered by different cloud providers.

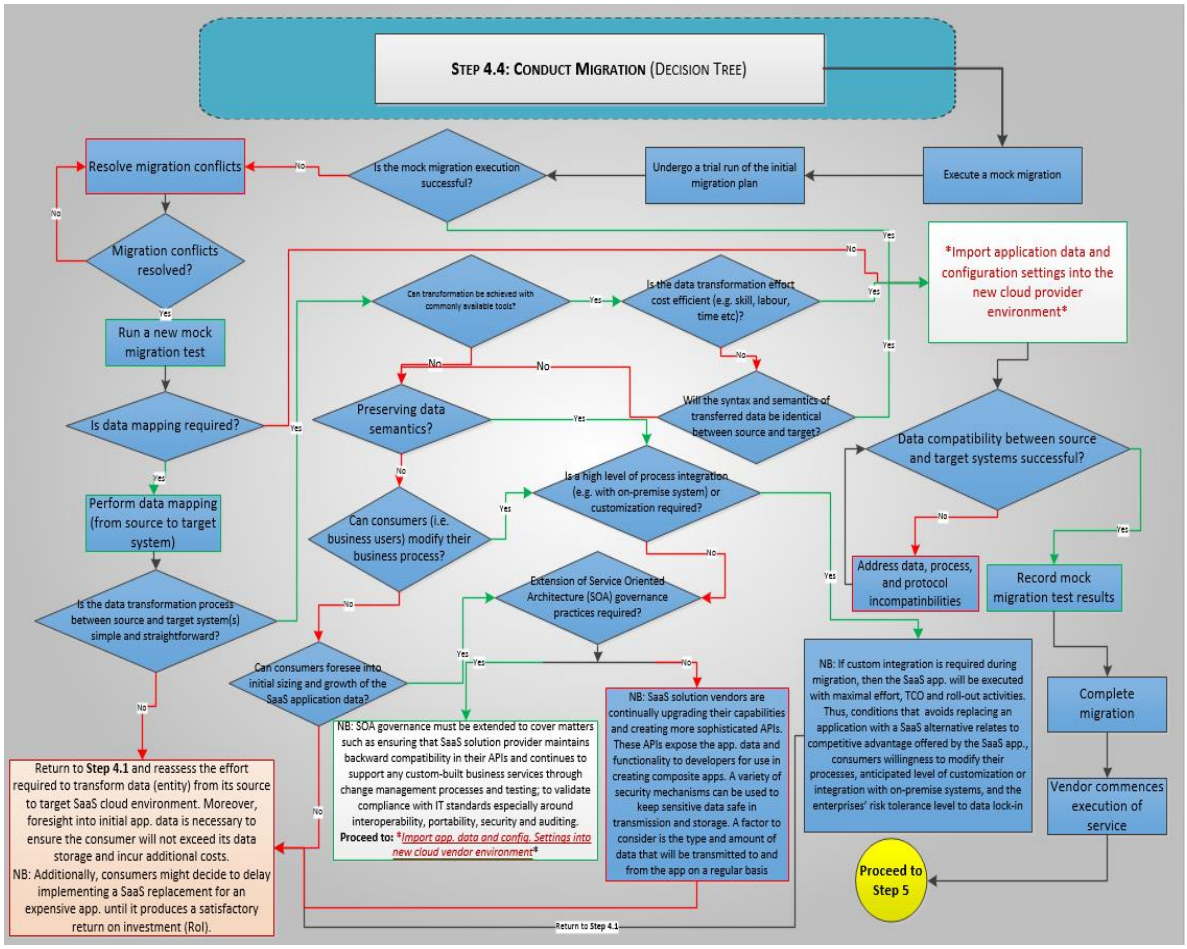


Figure 5.10-Decision Tree for Conducting a SaaS Migration (Step 4.4)

5.4.5 Step 5 – Service Testing and Validation

At this point, the migrated SaaS service is ready for test, validation, and use. The migration starts with a realistic test scenario *(i.e.* ***Step 5.5*** – see **Figure 5.11***)*, which is executed by employees of the cloud customer with real applications, but mostly in test environments and not in production environments. Tasks such as testing (i.e. interoperability, integration, security, auditability etc.), governance, organizational change, user training, SaaS risk assessment, multi-tenancy and elasticity analysis, validation and deployment of migrated application are performed. However, certain scenarios *(i.e. Step 5.2, Step 5.3, and Step 5.4)* testing cloud SaaS services make the cloud consumer also act in additional roles rather than just using the service, e.g. in the case of on-premise provisioning of cloud resources. This likely requires human capacity with sufficient knowledge and capabilities *(i.e. Step 5.1)* regarding cloud computing to be in-house to cope with the activities like manage, maintain, and/or operate the provisioned service. Determined by the outcome of the decision made in Step 5.1 an appropriate skill level regarding certain cloud activities is required. In case of the second decision step *(i.e. Step 5.2, for example)* this could be knowledge about integration, cloud performance and monitoring, interoperability, portability and compatibility to conduct the correct functional and non-functional testing. The last decision *(i.e. Step 5.5)* shows activities in the area of cloud service provisioning and validation, where operating and managing of the cloud service or the on-premise system infrastructure has to be dealt with by the staff of the cloud consumer.

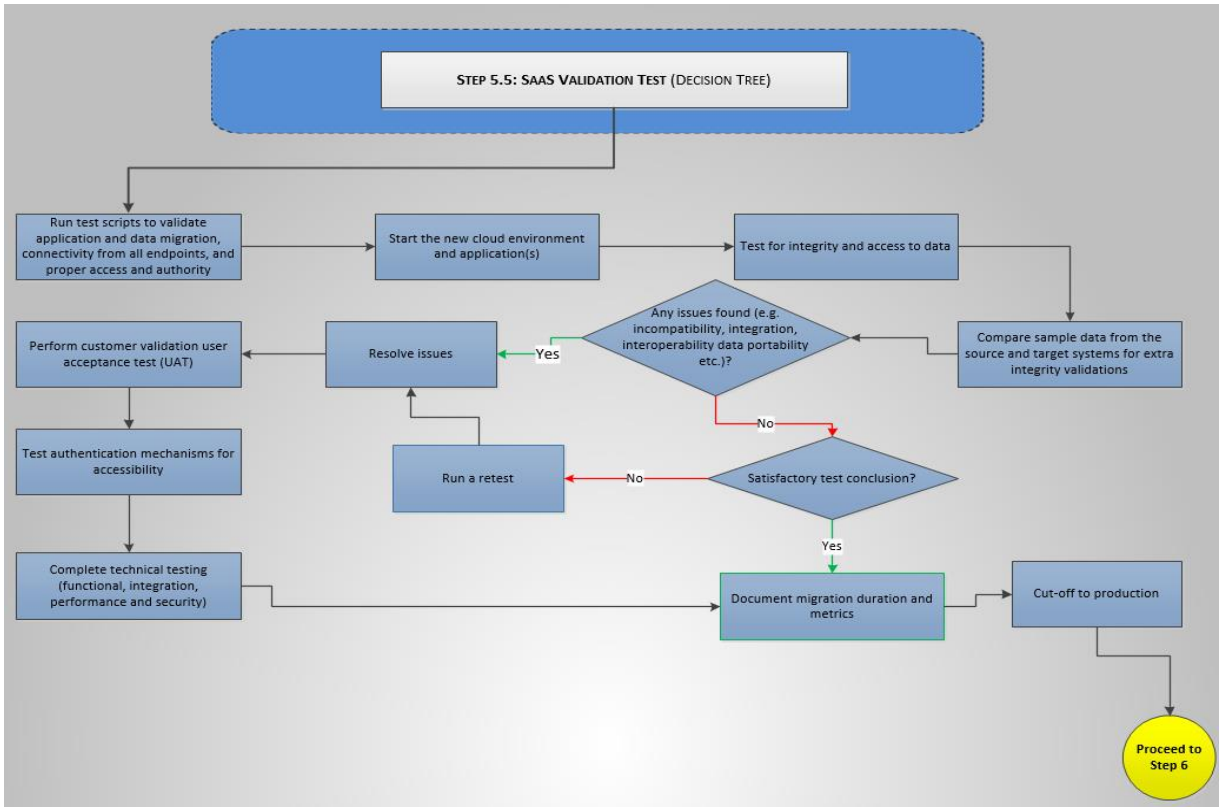


Figure 5.11-Decision Tree for Validating SaaS Migration (Step 5.5)

5.4.6 Step 6 – Service Operation and Optimization

This operation and optimization step is a steady situation where the cloud service customer mostly monitors *(*see **Figure 5.12** – *i.e.* ***Step 6.5)*** the procured service to ensure the quality of the IT-Service provision is sufficient. Measures describe in ISO 900 (Quality Management) and ISO 27000 (Information Security Management) can be applied here to guaranty the required service quality. Independent audit tasks can be performed in this step to guarantee the defined service quality.

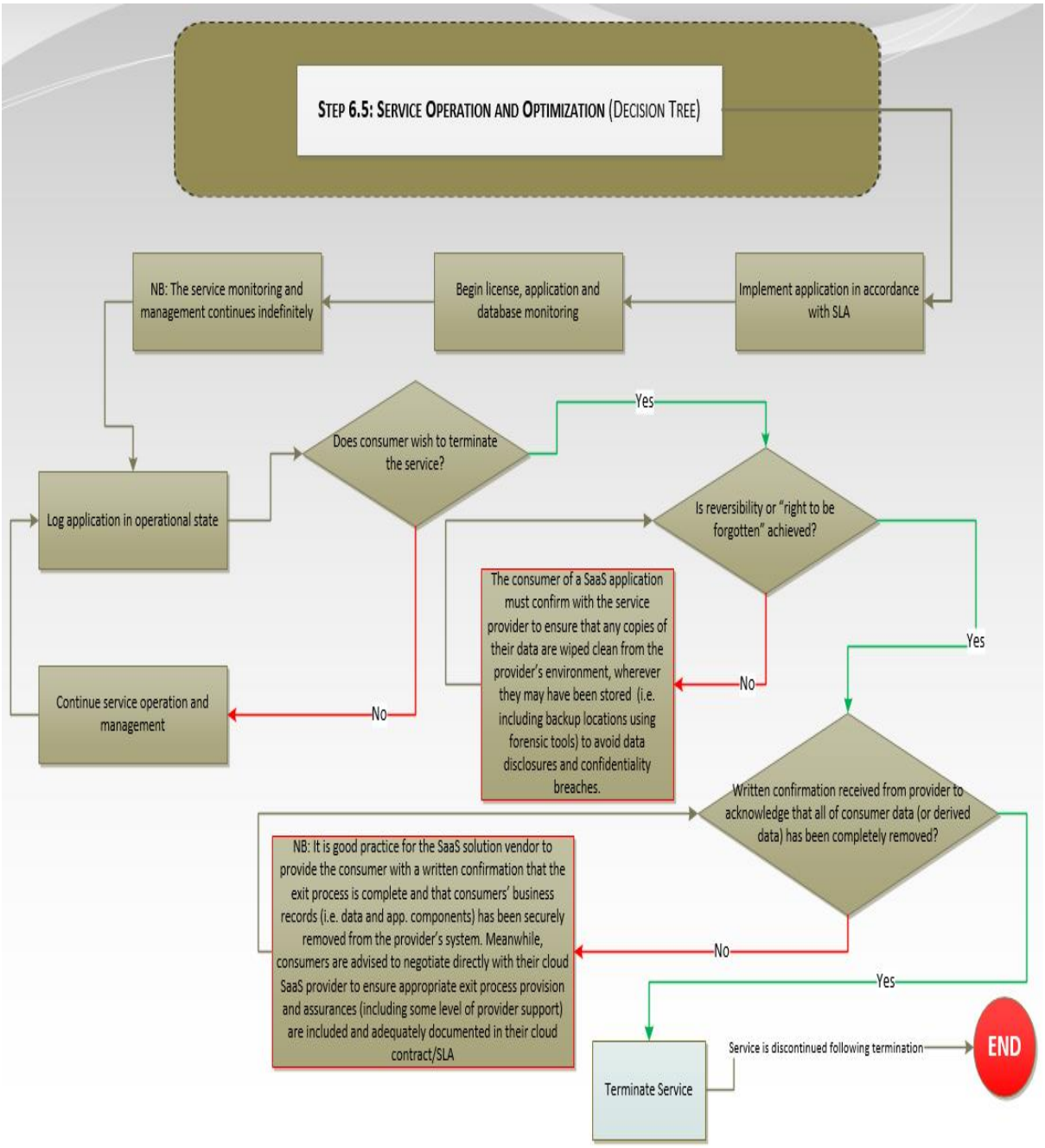


Figure 5.12-Decision Tree for Service Operation and Optimization

5.4.7 Optional Step – Service Termination or Rollback

Even when the cloud SaaS service is in a steady operational state, the customer might want to have a backup strategy in case things change in the future. The termination step is necessary under two main consideration(s): 1) that the rollback to internal IT-service provisioning; and 2) the change of the cloud service provider is not under consideration by a cloud customer. Often economic reasons or insufficient service provisioning leads a decision to change the IT-service provisioning that might lead to leaving the actual provider. Thus, an intensive preparation makes a change of cloud providers safer and more secure.

5.5 Relationship(s) between Steps, Tasks and Outcomes within the Framework

In this section, we discuss how the six main decision steps (1–6) are connected to each other within the framework. The focus is to identify "if" a certain decision step either influences (***I***) or determines (***D***) another step?

5.5.1 Influences and Relations with Decision Step 1

All decisions in Step 1 are strongly related within their sub-processes (i.e. tasks) and corresponding activities as well as to other steps in the framework, and predominantly other steps are influenced by the decisions made in Step 1. Within this step, all tasks and supporting activities are influenced by each other except for Step 1.5 which determines other core decision steps 2 through Step 6. It is expected that based on the evaluation report of SaaS risks events and levels, the outcome of Step 1.5 would influence the decision to either avoid migrating (i.e. replacing with proprietary cloud SaaS solutions) or perhaps, determine if the risk of lock-in to the SaaS solution is high; thus, making it expensive and disruptive to migrate (in future) from one vendor solution to another in the cloud. However, the outcome of Step 1.5 is what determines if the migration planning should proceed further to other steps consecutively. For example, an overview of relationships between the decisions and outcomes investigated in this step is represented in a decision-tree depicted in **Figure 5.7**.

5.5.2 Influences and Relations with Decision Step 2

Decisions, tasks and supporting activities in Step 2 are not closely related to each other but are intrinsically harmonious to other tasks within this step, as well as other steps in the framework by comparison to those relations discussed in Step 1. In this step, Step 2.1 through Step 2.3 are closely related to each other, however decisions made in Step 2.1 will determine the activities to be performed in Step 2.3. While these relations may depict a weak interdependence between decisions in Step 2, the influences nonetheless are very strong. For example, Step 2.1 and 2.3 are related but are mutually influenced by the outcome of Step 2.2 since due diligence can be performed independently

of Step 2.1 and 2.3 to proceed to the next decision Step 2.4. Moreover, defining criteria for using services of a cloud computing vendor and then evaluating the potential vendors against set criteria involves several trade-offs to be made by the cloud service consumer. In this case, the due diligence effort on possible vendors should be focused on evaluating those trade-offs, independently. In summary, with regards to Step 2.4, the outcome of decisions in this sub-step is what determines whether to proceed to Step 3 or perhaps return to Step 2.1 again.

5.5.3 Influences and Relations with Decision Step 3

Decisions made in Step 3 are principally influenced by tasks and supporting activities already performed in the preceding steps (1–2). Within Step 3, tasks and supporting activities are related since if a negotiation team is established to carryout negotiations (in the absence of a service broker), thus the drafting of ToS/SLA can be quickly processed and passed on for final review before proceeding to sign the cloud service contract agreement. In turn, the decisions made in Step 3.4 for example, clearly influences those made in Step 3.2 (in terms of renegotiation) and Step 3.5 (i.e. in terms of contract signing), because if the internal approval of draft ToS/SLA is granted in time, only then can the consumer proceed to review and exchange signed contract documents. However, if the internal approval returns negative then the consumer can either choose to re-instate contract discussions with selected vendor or perhaps try to renegotiate terms to suit the business needs before finally agreeing to sign the cloud service contract (Step 3.5). **Figure 5.9** shows a series of decisions and tasks to be performed in Step 3.5 and its relation to subsequent steps in the framework.

5.5.4 Influences and Relations with Decision Step 4

All the tasks and supporting activities within Step 4 are closely related to each other as well as to other steps within the framework. Decision Step 4.3 and Step 4.4 are influenced by decisions made in Step 4.2 since the selection of a chosen cloud migration scenario will help the cloud service consumer to better understand and provide the appropriate cloud resources for the deployment to take place. In this context, Step 4.1 determines the decisions and activities to be carried out in Step 4.2 through to Step 4.4, because the knowledge gathered from assessing the complexity of migration can be used also to determine the migration type, resources to be allocated, ease of implementation, and execution of migration plan. Generally, the outcome of the decisions made in Step 4.4 will determine the supporting activities and tasks performed in Step 5.

5.5.5 Influences and Relations with Decision Step(s) 5 and Step 6

Within Step 5 itself, activities performed and decisions made in Step 5.1 influences all other tasks in the framework. That is, Steps 5.2–5.5 are largely influenced and determined by decisions made in Step 5.1 because its only when an in-house SaaS team is built can the enterprise assign test and

validation roles to the organisation employee accordingly. Finally, in Step 6, a couple of relationships exist within the step itself and with other steps in the framework. Step 6.4 and Step 6.2 are both influenced by the decisions made in Step 6.1 since its only when the system has gone live can a cloud service user perform tasks such as monitoring, decommissioning, and organisational change management. Step 6.3 is influenced by Step 2.2 within the framework in that customer audit rights might have been covered during the due diligence process. On the other hand, decision step 6.5 (i.e. post migration support) is influenced only by Step 2.4. However, the type of post migration support in this case is not limited to only exit strategy or termination plan but also includes business continuity and plans to roll back to on-premise systems as and when needed. An overview of all relationships between the decisions and outcomes investigated in the proposed novel framework is presented in a tabular form in ***Appendix 5.***

5.6 Evaluation of the Proposed Six-Step Decision Framework for Cloud SaaS Migration

In this section, a set of key questions are used to evaluate the usability and effectiveness of the novel 6-step decision framework presented in the preceding section. Here, author start by discussing the procedure employed in evaluating the proposed decision framework to mitigate vendor lock-in risks in cloud SaaS migration. This proposal was evaluated by a group of IT practitioners, academics and cloud specialists with good experience of cloud-based services and migration. The evaluation focuses on confirming key objectives such as the appropriateness, importance, suitability and overall effectiveness of the six decision steps, supporting activities/tasks and outcomes within the framework. Furthermore, the evaluation data obtained during a six-month period (i.e. October 2016 – April 2017) provides useful insights into how effective generally the proposed framework is in terms of supporting and systematically guiding organisations' decision-making process for migration to cloud computing. In turn, its results should then provide a reasonable peer review of the 6-step decision framework to evaluate the suitability in tackling the vendor lock-in problem.

5.6.1 Evaluation Objectives

Prior to discussing the evaluation procedure, we first outline the measurable outcomes author aim to achieve in this evaluation process, with respect to the given objectives (i.e. **O.6**) of this PhD thesis specified in *Section 1.3*. These outcomes are the very things that constitute our evaluation objectives (EO) as listed below:

E01. Evaluate the **appropriateness** of each task/activity within the respective steps of the framework.

E02. Evaluate the **importance** of identified tasks/activities within each decision-step (1–6) in the framework.

E03. Evaluate the **suitability** of sample decision-trees within the respective steps (e.g. Steps 2.2 and 2.4) of the framework.

E04. Evaluate the **overall effectiveness** of the proposed cloud decision framework to avoid vendor lock-in risks.

5.6.2 Procedure

The procedure for this evaluation was performed by a Web-based survey tool (Survey Monkey, 2017). Prior to collecting raw (or source) data for the evaluation study, a pilot test of the questionnaire was administered to 10 PGR students to identify errors, avoid wrong design and predict possible problems. A complete list of questions used in the evaluation survey is attached in ***Appendix 6***. Conducting the survey with a questionnaire is a systematic and standard research procedure for data collection on large study population. Hence, data collection for this evaluation via Web-based questionnaires generally improves objectivity, generalizability, and reliability of the research findings. The questionnaire has been designed respecting conventional wisdom in terms of creating questionnaire like group questions on the same topic and processes them from general to specific, to address the stated evaluation objectives in *Section 6.9.1.* The questionnaire design which consists of 26 questions was developed following the guidelines prescribed in Shared Assessment Agreed upon Procedures and Standardised Information Gathering Questionnaire (SIG, 2010). A mix between open- and close-ended questions was used in the questionnaire. Participants in the survey varied between IT professionals, managers, cloud architects, consultants and developers with expertise in cloud computing.

- ***Descriptive Analysis Method***

Most items in the survey questionnaire were rated on a 0–4 Likert scale. To describe the questionnaire evaluation responses and thus the attitude of the respondents toward each question they were asked in the questionnaire, the mean and standard deviation were estimated. While the mean shows the central tendency of the data, the standard deviation measures the dispersion which offers an index of the spread or variability in the data (Sekaran and Bougie, 2013). In other words, a small standard deviation for a set of values from the evaluation result reveals that these values are clustered closely about the mean or located close to it; while a large standard deviation indicates the opposite. The benefit of using a Likert scale in the questionnaire is that it gives respondents several alternatives if they are unsure of their commitment to a stance (Sherif & Sherif, 1967). However, the level of each item was determined by the following formula: (highest point in Likert scale - lowest point in Likert

scale) / the number of the levels used = (4-0) / 5 = 0.80, where 0-1.80 reflected by "Not appropriate/important", 1.81-2.60 reflected by "slightly appropriate/important", 2.61-3.40 reflected by "moderately appropriate/important", 3.41-4.20 reflected by "very appropriate/important", and 4.21-5 reflected by "absolutely appropriate/important". In agreement with the employed rating scale, a meta-analysis by Nielsen and Levy (1994) also confirmed that 80% of the number of points in a Likert-type scale is a good point to evaluate performance measures in questionnaires, where participants respond to a prompt statement by selecting a position on a labelled response scale.

- ***Assessment of Statistical Significance of the Survey Participants***

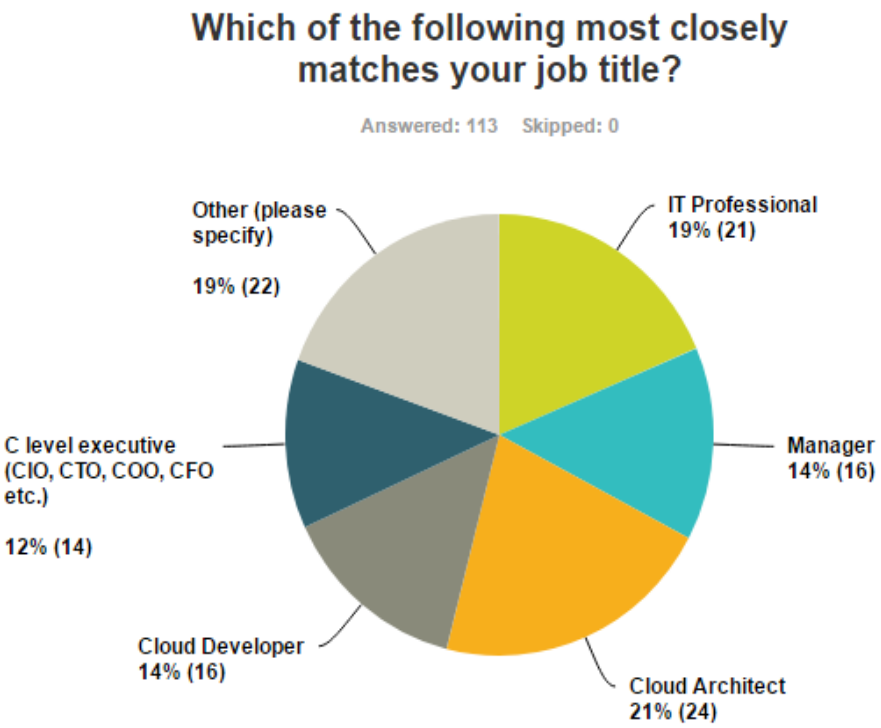
The word significant as used in everyday terminology means *"important or meaningful,"* whereas, in survey analysis and statistics, significant means "*an assessment of accuracy.*" In this section of the thesis it means that the framework evaluation survey results are accurate within a certain confidence level and not due to random chance. Being that the survey sample or participant group was based on a random selection from a known population (i.e. target audience as per IT practitioners, cloud specialists, developers, managers, C-level executives etc.), statistical significance was calculated in a straightforward manner (as shown in ***Appendix 7***). However, two main primary factors considered by the researcher in this assessment of statistical significance are, 1) the aspect of causation vs. correlation, and 2) the representativeness of the research sample, based on the sample size – that is, to what extent the participant group who took part in the survey represent the total population of people and organisations (i.e. enterprises and SMEs) about whom author draws conclusions on to 'represent' the wider enterprise population. With regards to the former, causation is when one factor causes another, while correlation as the latter is when two variables move together, but one does not influence or cause the other. Hence, to further examine the relationship between variables in this evaluation survey, author considered it useful to perform ANOVA analysis (as shown in ***Appendix 7***). Analysis of variance (ANOVA) is similar to regression in that it is used to investigate and model the relationship between a response variable and one or more predictor variables. However, ANOVA as used within this chapter differs from regression in two ways: the predictor variables tend to be categorical. In effect, analysis of variance extends the two-sample t-test for testing the equality of two population means to a more general null hypothesis of comparing the equality of more than two means, versus them not all being equal.

Specifically, in descriptively analysing the evaluation survey data for statistical significance, author was interested in knowing what factors most impact participants' (i.e. stakeholders and enterprise decision-makers) satisfaction with the proposed decision framework: Is it the logical order or sequence of the identified cloud migration decision steps? Is it the importance or appropriateness of each decision step and tasks with their corresponding activities? Is it the sample decision tree? Or, is it the overall effectiveness of the framework in terms of its comprehensiveness and multi-

dimensionality? Because author wishes to test the equality of means and to assess the differences in means, the one-way ANOVA procedure with multiple comparisons was used in this analysis to: determine whether the means of two or more response groups (i.e. for each evaluated decision step(s), tasks, and supporting activities within the proposed framework) differ; obtain a range of values for the difference between each pair groups; graph evaluation survey data accordingly. Therefore, the purpose of assessing the statistical significant of survey respondents in this thesis was to determine if one or more decision steps and tasks within the framework was more effective than the others in avoiding vendor lock-in and/or improving organisations' cloud adoption and migration decision-making process. Hence, using ANOVA in this chapter of the PhD thesis have enabled the researcher to determine whether and to what extent satisfaction with these questioned attributes of the proposed novel 6-step decision framework contribute to overall IT practitioners and academia satisfaction. In turn, this descriptive statistical assessment provides powerful insight into what aspects of the decision framework might require future research work and directions.

5.6.3 Participant Group

According to Zikmund (2000), target population is the entire group of subjects of interest who are defined by the research objectives. However, there is usually a considerable difference between the population that a researcher is attempting to study and those available for sampling (Hair et al. 1992). The evaluation survey in this PhD study polled senior IT practitioners, cloud specialists and business decision-makers in large enterprises, small to medium sized enterprises, academia and public sector organisations etc. These participants' group were purposefully targeted as respondents in this study because they are in a better position to make purchasing decisions as well as understand the current enterprise cloud initiatives, IT operations and future trends of the firms. A total of 230 participants were invited to participate in the survey on-line. In return, researcher received 117 responses from different firms, including 4 responses that were rejected because they contained errors and/or partial responses. Overall, there were a total of 113 complete usable responses received which constituted a satisfactory completion rate of 49%. Further evaluation of the survey findings takes into account only the complete responses to the questionnaire to gain consistency in the number of responses through all survey questions. However, incomplete responses have been omitted from the thorough analysis presented herein. The distribution of the survey participants is shown in **Figure 5.13**. As can be drawn from the figure below, the study samples were slightly dominated by cloud architects (21%), IT professionals (19%) and others (19%).



Answer Choices		Responses	
IT Professional (1)		19%	21
Manager (2)		14%	16
Cloud Architect (3)		21%	24
Cloud Developer (4)		14%	16
C level executive (CIO, CTO, COO, CFO etc.) (6)		12%	14
Other (please specify) (7)	Responses	19%	22
Total			113

Figure 5.13-Group of Survey Participants

Fortunately, managers (14%), cloud developers (14%), and top IT executives (12%) were also accounted for in the survey considering that they have significant influence over the cloud computing purchase process than business leaders. Simple socio-demographic information was also requested, in which IT board area, degree completed, and what level of decision-making authority respondents have in purchasing IT-related services for their organisations. **Figure 5.14** presents a socio-demographic profile of survey respondents, many of whom have completed or achieved an associate degree, and have a good experience with cloud computing migration and SaaS adoption strategy. As illustrated in the figure, most sample participants fulfil the following criteria: (39%) have completed a graduate or professional degree; (19%) hold a PhD, while the lesser minority have either some bachelors (18%) or associate (17%) degrees. However, in terms of respondents reporting personal involvement and authority in the decision-making process for cloud solutions at their respective organisations, as

depicted in **Figure 6.9,** the majority (44%) have a significant influence, while 34% have minimal decision-making authority, followed by the lesser 15% of respondents who have final decision making authority (whether as a group or individually) for purchasing IT related services within their respective organisations. These survey results represent the professional background and opinions of IT decision makers whose organisations have made cloud investments or have plans to do so. Since, a greater commitment to cloud computing requires changes within the IT and business operations function of an organisation. These commitments, however, pose challenges related to vendor lock-in or dependency, compliance and governance issues, security and changes in the roles and responsibilities of employees working in the business and IT functions of the organisation (Rajendran, 2013). Hence, in this evaluative survey, it was important to include questions that investigates participants job roles. This was done in an effort to collate the right information from the correct employees that practically deal with the challenges organisations moving to the cloud face on a daily basis. Therefore, to assess each participants' level with cloud computing and IT services in general, in **Figure 6.10**, the survey result found that while (38%) of respondents had an excellent experience with IT services, 62% have a good experience with adoption of cloud-based SaaS services, followed by the other 59% and 55% respectively, with either a good experience with cloud computing or with cloud computing migration. Overall, this demographic information proves that respondents of the survey have the necessary knowledge and experience to give valuable insights to the novel 6-step decision framework.

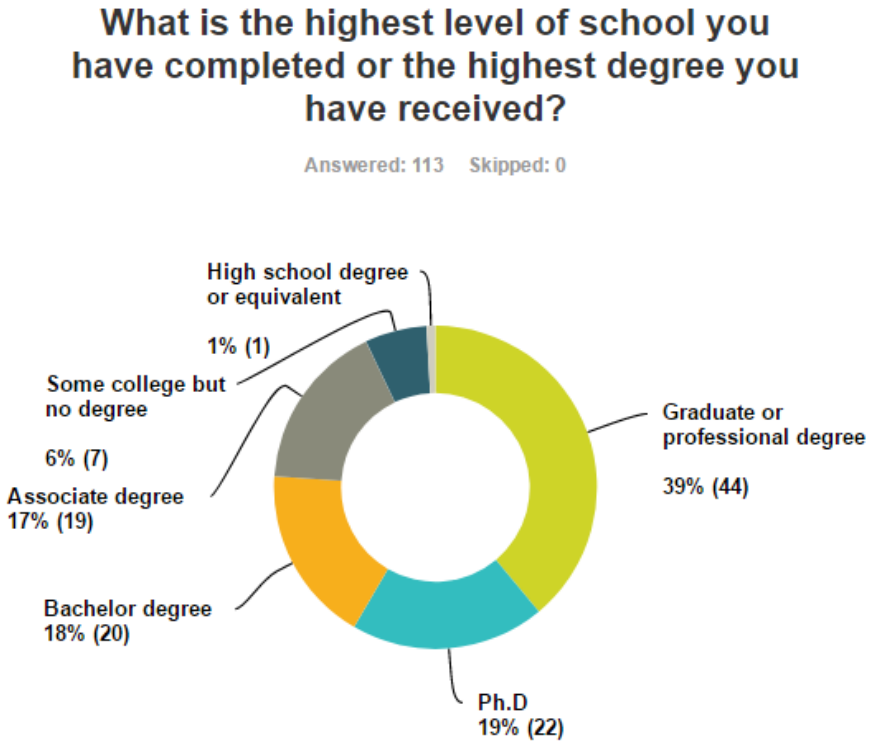
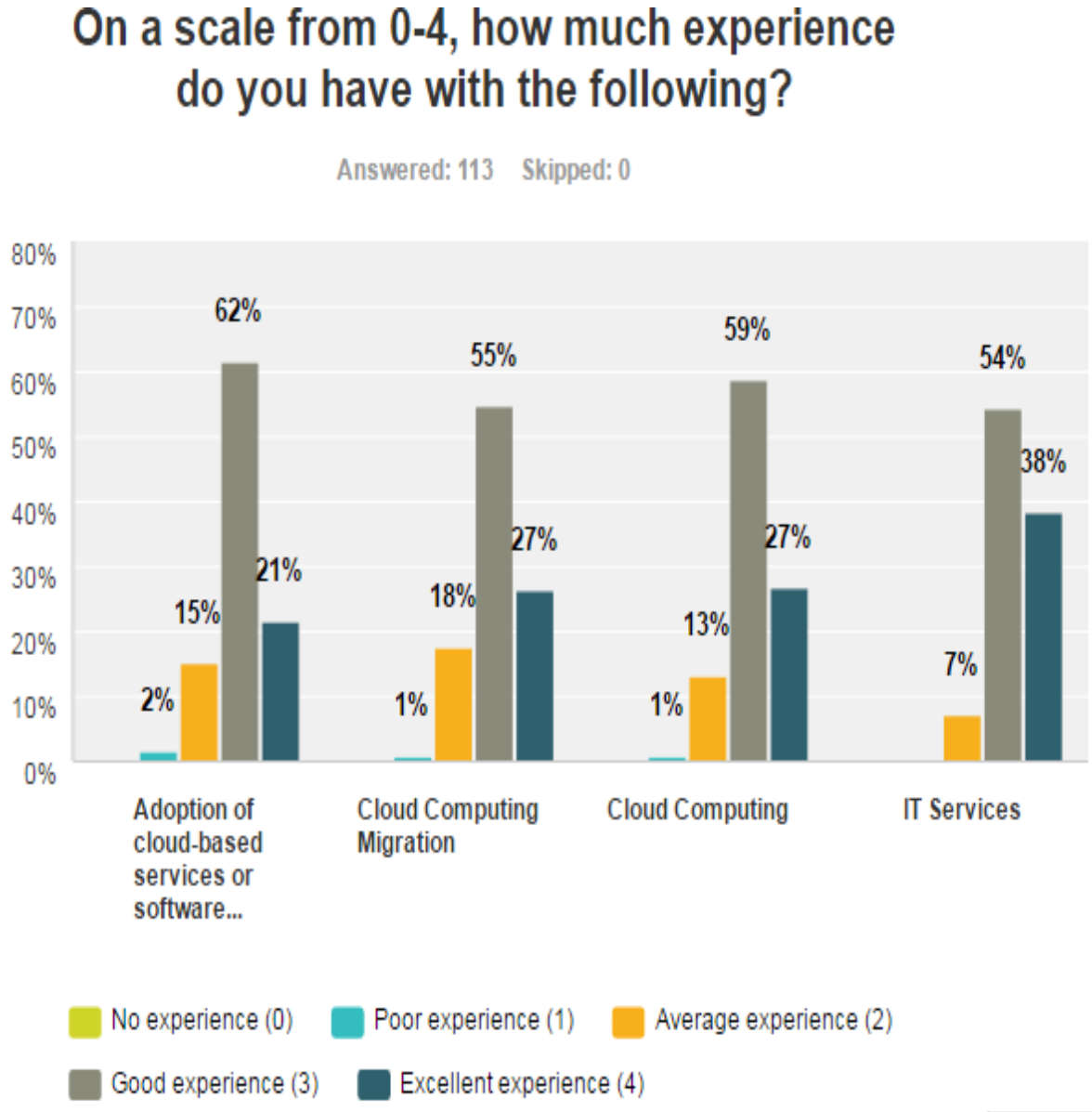


Figure 5.14- Socio-demographic Profile of IT Practitioners

Answer Choices	Responses	
Final decision-making authority (individually or as part of a group) (1)	15%	17
Significant decision-making or influence (individually or as part of a group) (2)	44%	50
Minimal decision-making or influence (3)	34%	38
No input (4)	7%	8
Total		113

Figure 5.15- Assessing Decision-Making Capacity



	No experience (0) (1)	Poor experience (1) (2)	Average experience (2) (3)	Good experience (3) (4)	Excellent experience (4) (5)	Total	Weighted Average
Adoption of cloud-based services or software applications	0% 0	2% 2	15% 17	62% 69	21% 24	112	3.03
Cloud Computing Migration	0% 0	1% 1	18% 20	55% 62	27% 30	113	3.07
Cloud Computing	0% 0	1% 1	13% 15	59% 66	27% 30	112	3.12
IT Services	0% 0	0% 0	7% 8	54% 61	38% 43	112	3.31

Figure 5.16-Respondents Experience with Cloud Computing and IT Services

5.7 Discussion of Significant Statistical Findings

This section provides an overview of key findings from the evaluation survey. The data results from the evaluation survey were imported from a survey tool (Survey Monkey, 2017) into Microsoft Excel (2016) for data cleansing, and later into Minitab 17 (2017) for statistical data analysis. The 6 main decision steps (*i.e.* ***Steps 1–6***) and 28 tasks (i.e. ***Steps 1.1, 2.1, 3.1–6.6 etc.***) with supporting activities were measured using a five-point Likert scale to investigate how these components vary across different participant's groups, decision steps, and tasks identified to avoid vendor lock-in challenges in the cloud migration process. **Figure(s) 5.17–5.35** summarises the evaluation questionnaire survey results with respect to the objectives of appropriateness, importance, suitability, and effectiveness of the proposed decision framework. Typically, in the questionnaire survey, a respondent is asked to indicate his or her level of agreement to a statement regarding the framework according to the following Likert scale response variables. Note all numeric results in this section respect this rating scale, unless otherwise stated.

Rating Scale for ***Appropriateness***:	Rating Scale for ***Importance*:**
0 = Not appropriate,	0 = Not at all important,
1 = Slightly appropriate,	1 = Slightly important,
2 = Moderately Appropriate,	2 = Moderately important,
3 = Very appropriate,	3 = Very important,
4 = Absolutely appropriate	4 = Absolutely important

Now, to further reiterate, the framework is evaluated to yield concrete statistical confirmation in terms of the following questions below. Note, such 'how' questions outlined are particularly suitable for our framework proposal evaluation as they involve direct feedback from participants in the context of their day-to-day job.

- Is the logical order of the steps within the framework appropriate? Note, by logical order we mean how reasonable or sensible the sequence of steps within the framework happens or should happen in typical cloud migration.

- How important is each step to you in a cloud SaaS migration? Note, by importance we mean how relevant a step is for you in a typical cloud migration. The more you feel the step is important, the higher you would rate it or vice versa.

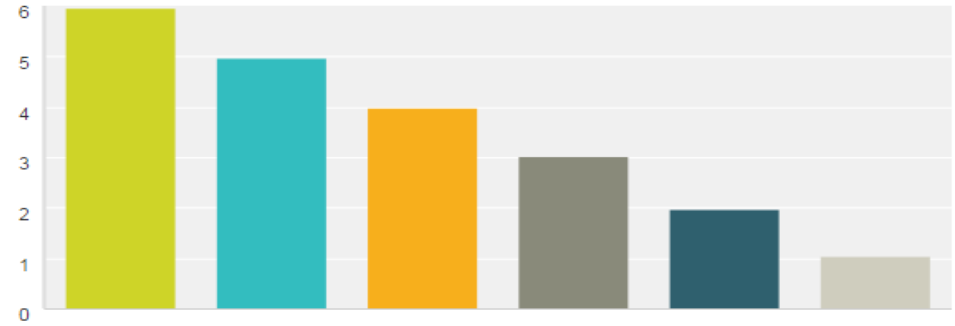
- Overall, how **effective** would you evaluate the framework to support informed decision-making process for organisations' migration to cloud computing.

5.8 Logical Order and Sequence of Decision Steps

The adoption of, and migration to, cloud computing requires a comprehensive decision-making framework, taking a few vendor lock-in aspects into careful consideration. Existing frameworks and methods of migration, however, limit decision making to the relative costs and security of cloud computing, but do not take a broader range of lock-in criteria (or elements) into account. In this evaluation survey analysis, we report on the result of our proposed 6-step decision framework for cloud SaaS migration. The logical order and sequence of steps within the decision framework allow organisations to determine what cloud-based SaaS solution best suits their needs by evaluating and ranking SaaS vendors and service alternatives based on multiple criteria to avoid vendor lock-in risks, prior to migration. To obtain quantifiable facts in this respect, IT practitioners who took part in the survey were asked to rank the sequence of steps identified in the proposed decision framework presented to them in a random order of choices. **Figure 5.17** presents the analysis of the respondents, and as shown with annotations, it appears that there is a high level of acceptance with the frameworks logical order (note, the green arrow in figure below depicts the descending order of steps based on their average weighted mean values). However, it should be clear from the figure that only 2% (i.e. n=2) respondents considered re-ordering the logic of step 3 and step 4 alternatively. This finding seems somewhat counter-intuitive in the sense of a typical cloud implementation scenario. For instance, how do you design and execute a migration plan without firstly identifying and contracting with the potential vendor – whose operating environment is the target platform. What this interprets is that, perhaps, those respondents considered the step labelled "design and execute migration plan" to proceed first in the frameworks hierarchy before the "contract negotiation and SLA agreement" step. Likewise, 2% of participants also re-ordered the sequence of step 5 and step 6 – making the "service operation and optimization" step to come before "service testing and validation design". A possible implication of this finding for the participants who preferred the alternative logic is statistically insignificant in comparison to the majority (98%) of participants who agree with the overall sequence of steps within the proposed decision framework. Thus, no further investigation is required in this respect. Moreover, the steps participants re-ordered were related to specific phases (i.e. between Phase 2 and Phase 3) in the proposed framework for avoiding vendor lock-in risks in the cloud SaaS migration process. Nonetheless, author further investigated participants' responses to see if the logical order of decision steps in the framework were appropriate (*see* **Figure 5.18**).

The following are steps within the framework that organisations should go through when migrating to Or switching cloud Software-as-a-Service (SaaS) providers to avoid vendor lock-in. If you do not agree with the logical order, please indicate the order that you wish to see in the framework.

Answered: 112 Skipped: 1



	1	2	3	4	5	6	Total	Score
Step 1 - Initial Migration Planning	98% 110	2% 2	0% 0	0% 0	0% 0	0% 0	112	5.98
Step 2 - Vendor Evaluation and Selection	1% 1	98% 110	0% 0	0% 0	1% 1	0% 0	112	4.98
Step 3 - Contract Negotiation and Service Level Agreement (SLA)	1% 1	0% 0	97% 109	2% 2	0% 0	0% 0	112	4.00
Step 4 - Design and Execute the Migration Plan	0% 0	0% 0	2% 2	98% 110	0% 0	0% 0	112	3.02
Step 5 - Service Testing and Validation	0% 0	0% 0	0% 0	0% 0	98% 109	2% 2	111	1.98
Step 6 - Service Operation and Optimization	0% 0	0% 0	1% 1	0% 0	2% 2	97% 109	112	1.04

Figure 5.17-Sequence of Steps in the Framework

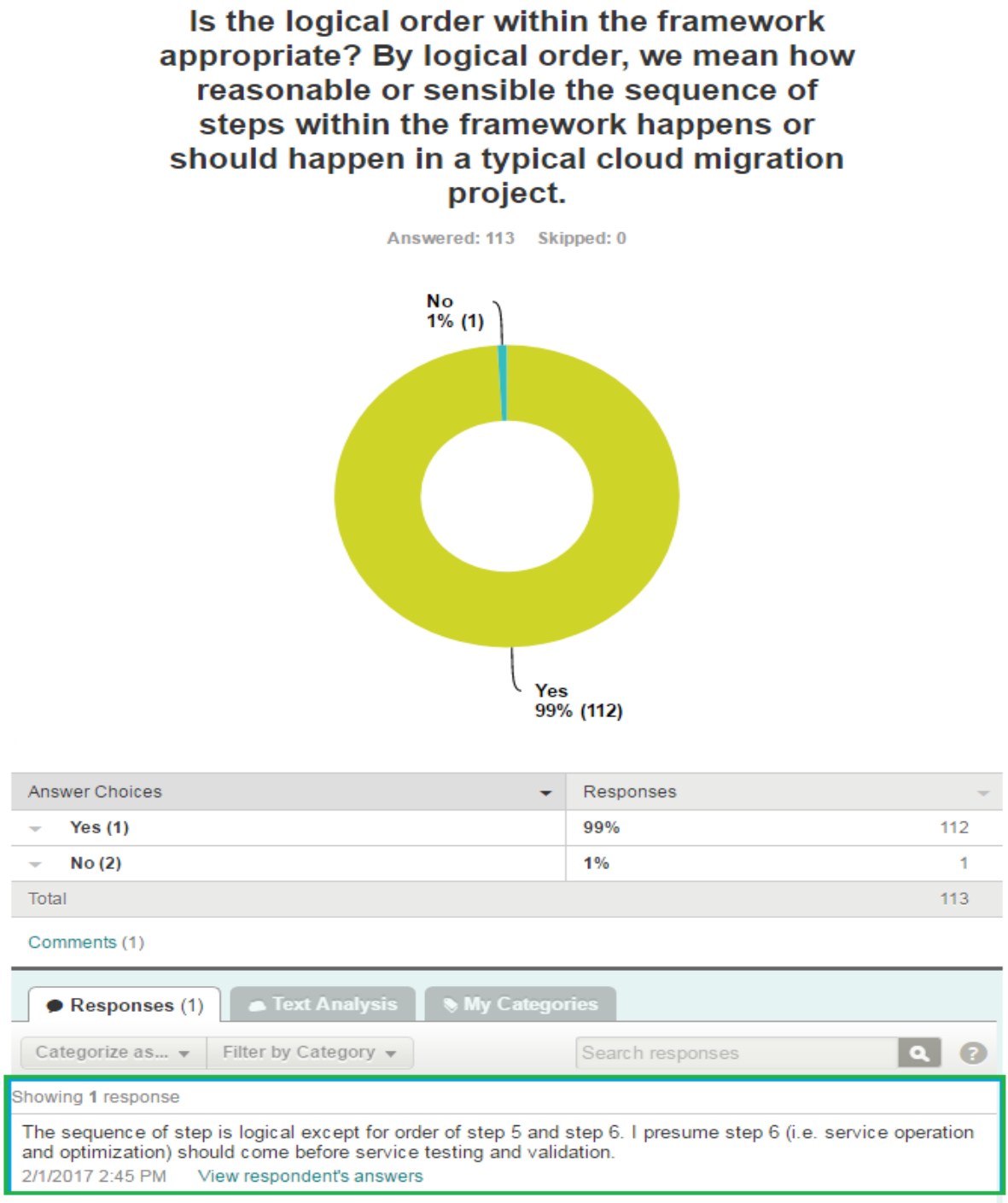


Figure 5.18-Logical Order of Steps

Figure 5.18 above shows that the greater majority (99%) of IT managers and decision–makers concur that the logical order of the proposed novel framework is appropriate – that is, the sequence of steps and supporting activities are ordered in a way that is relevant or suitable for avoiding vendor lock-in risks in cloud migration. However, only one respondent (i.e. 1%) believe the logical order of steps within the framework were consistent. The reason for such negative response is highlighted in green in the figure above, which is also in agreement with the discussion presented earlier in the preceding paragraph.

5.9 Appropriateness and Importance of the Identified Cloud Migration Decision Steps (1-6) to Avoid Vendor Lock-in

Vendor lock-in, as thoroughly investigated within this thesis, is a problem that has the potential to obstruct portability and interoperability, thus making it a significant source of frustration for organisations looking to take advantage of the many proven benefits of cloud computing. Therefore, a decision framework incorporating tasks to facilitate informed decision-making is necessary to support a careful, systematic plan for cloud migration. This is important because when cloud users intend to migrate to/from the cloud, or perhaps replace in-house systems with cloud-based services, such frameworks would enable them to understand the lock-in risks and needs of both the application and user when adapting to the cloud environment, and how cloud provider's supports those needs. In this vain, the six main migration decision steps identified in the novel framework are assumed to be of equal importance and propriety when planning for a successful systematic migration with minimal vendor lock-in risk. However, to assess the suitability of these steps in a typical cloud migration project and to specifically address ***E01*** and ***E02***, participants were asked to rate the *appropriateness* **(***see* **Figure 5.19)** and *importance* **(***see* **Figure 5.20)** of these steps collectively.

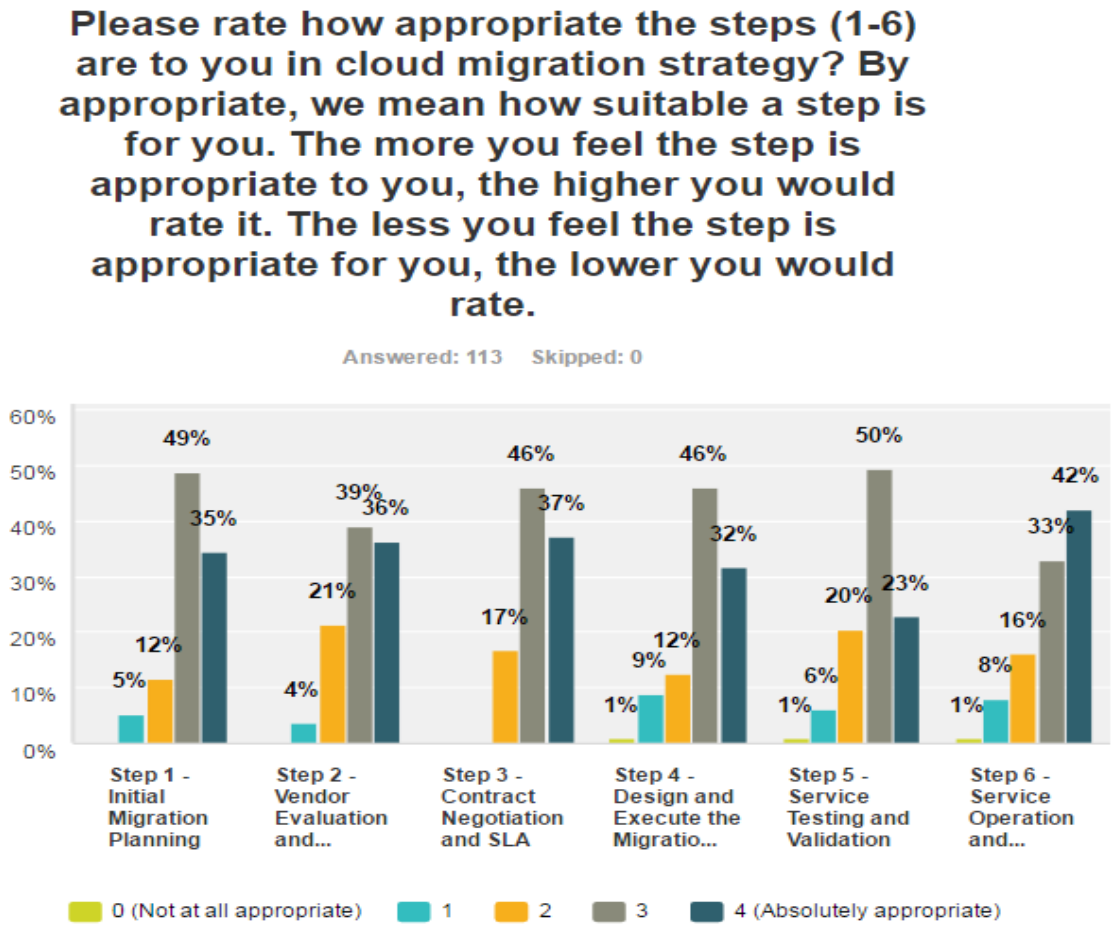


Figure 5.19-Appropriateness of Decision Step(s) 1 – 6

As shown in **Figure 5.19**, the result is evenly distributed across the different steps. However, using an average rating of 4.06 out of 5, based on the weighted average computation for all steps in the framework. On average, the results show participants rated "step 3 – Contract Negotiation and SLA" (4.20) to be absolutely more *appropriate* than "step 1 – Initial Migration Planning" which scored an average ratings of 4.12 out of 5 in comparison with the (4.08) weighted average ratings for "step 2 – Vendor Evaluation and Selection". However, it should be noted that "step 5 – Service Testing and Validation" scored the lowest weighted ratings with 3.88 out of 5. Based on these analyses, it inferred that IT decision-makers and enterprise stakeholders, who consider vendor lock-in a challenge in their organisations, value the SLA and contract negotiation process (in phase 2) more than even designing and executing the initial migration plan (3.99).

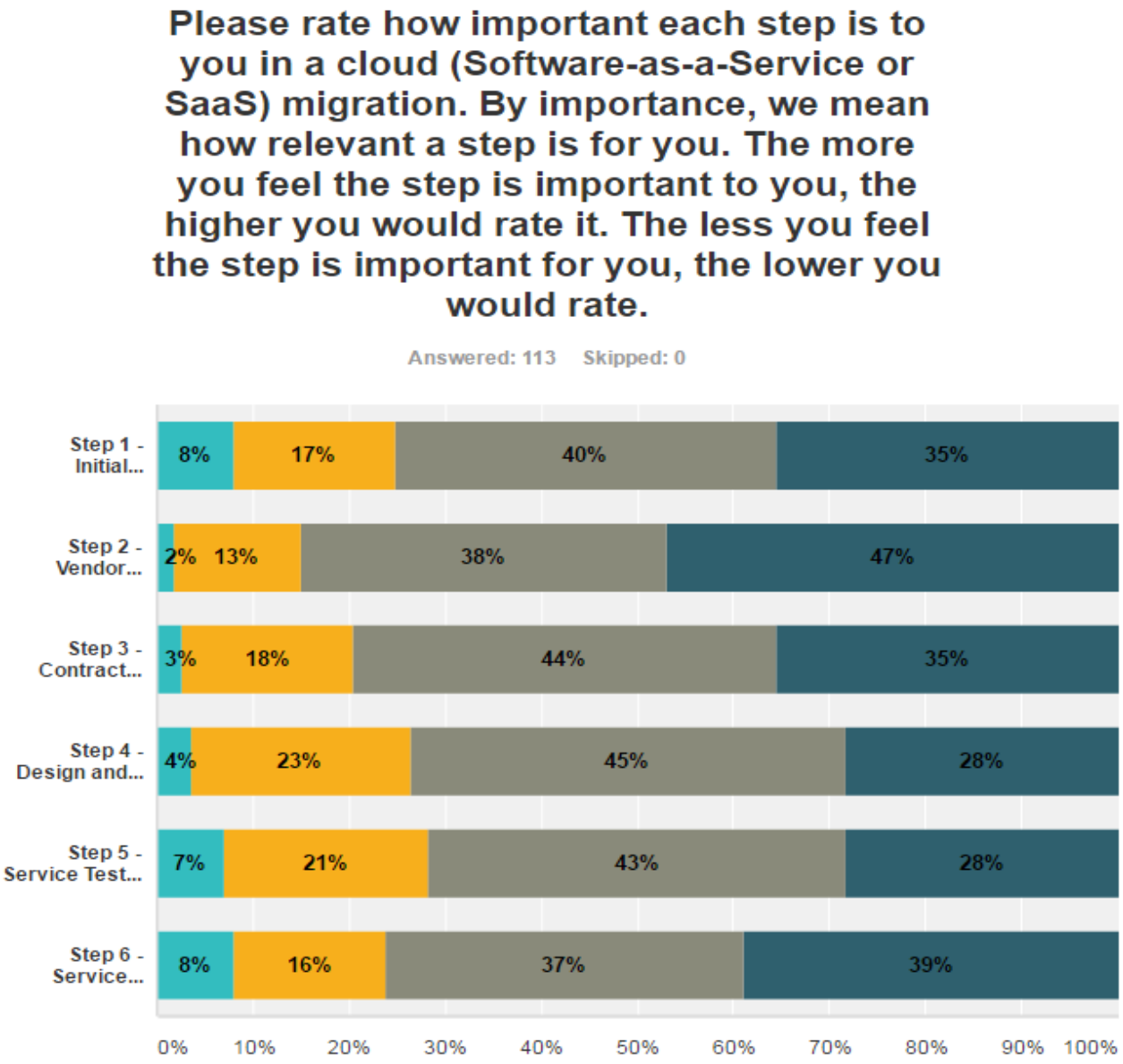


Figure 5.20-Importance of Decision Step(s) 1 – 6

This result is insightful in the sense that: firstly, it nullifies the earlier negative findings for re-ordering logical order and sequence of steps in the frameworks (*refer to* **Figure 5.17**) and; secondly, it further reinforces the need for consumers to develop and maintain a good vendor relationship management skill as well as effective and compliant contract strategies prior to procuring cloud-based services or moving between different cloud vendor environments. Furthermore, since cloud computing involves two organisations – i.e. the cloud service user and the cloud service provider – interoperability, portability and security requirements and responsibilities of each party must be made clear. Quite often, this is usually done by means of SLA which applies to the services provided and the terms of the service contract between the customer and the provider. Currently, there are few standard initiatives taking a closer look at common metrics and management approaches for interoperable and portable cloud SLAs, including QoS and security metrics.

On the other hand, **Figure 5.20** shows that the most *important* decision steps considered by participants in the study are "step 2 – Vendor Evaluation and Selection (4.30)", "step 3 – Contract Negotiation and Selection (4.12)" and "step 6 – Service Operation and Optimization (4.07)". Similar to the survey result in **Figure 5.19**, herein service testing and validation was also rated the lowest with a weighted average of (3.93). Again, this highlights the importance of the vendor selection and evaluation process when contracting with existing cloud providers. This step (2) is highly essential when planning for a successful cloud implementation to avoid the potential risks of single provider lock-in, since most cloud vendors still use proprietary APIs and file formats as way of lock-in customers to their services. Nonetheless, the effort required for re-engineering an application or data in order for it to be ported to another providers cloud environment (or back on-premise) although can be discouraging for customers, but such efforts can still be minimised if the right vendor had been evaluated and selected in the first place. In subsequent sections, author will deliberate on the *propriety* and *importance* of each task within the six main decision steps.

5.10 Importance of each Task in Decision Step(s) 1-6

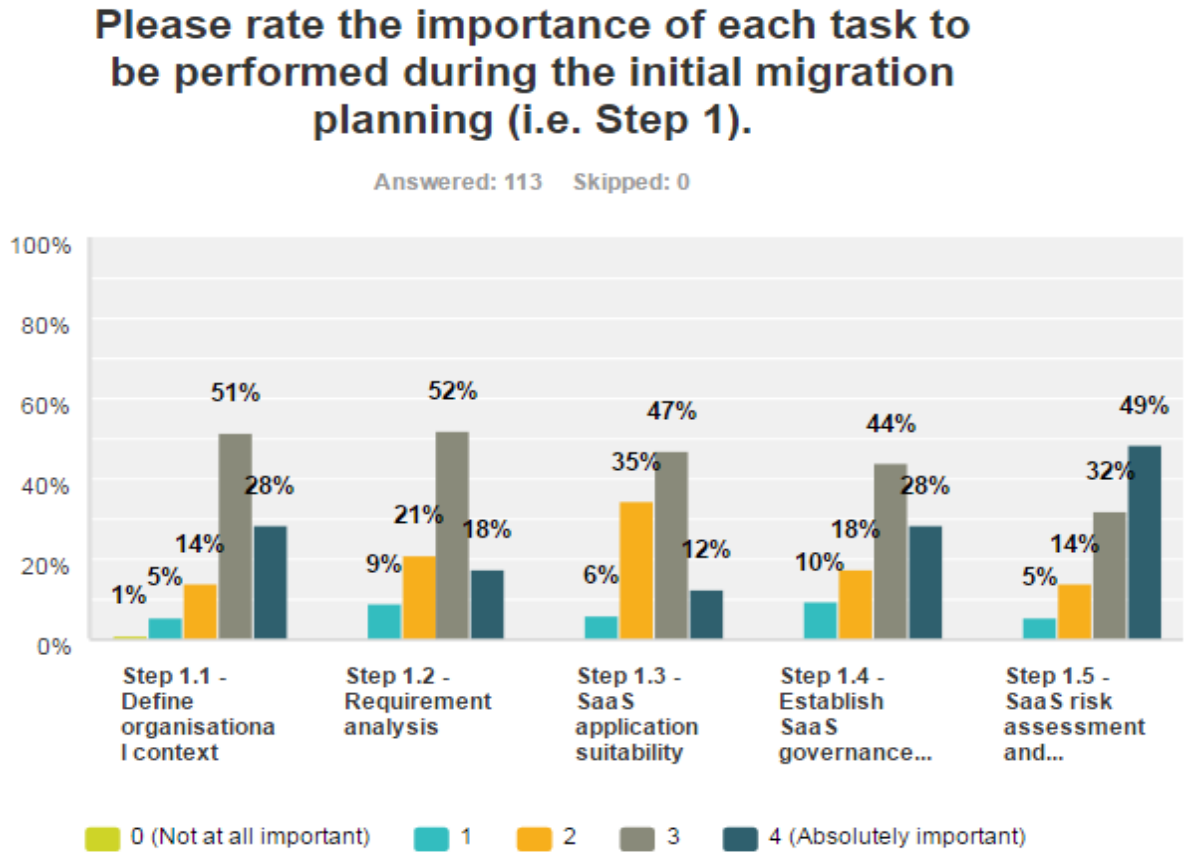
In this section, the discussion and evaluation of tasks within each main decision step have been categorised succinctly into different phases of the proposed framework as presented below.

5.10.1 Phase 1 – Service Selection and Evaluation

- *Tasks within the Initial Migration Planning **Step 1***

In **Figure 5.21**, participants were asked to rate the importance of the tasks identified in Step 1. The survey findings according to the figure below show that with an average rating of 3.92 out of 5, "step 1.5 – SaaS risk assessment and mitigation" was perceived by the majority (4.24) as the most *important* task, next to step 1.1 – "Define organisational context (4.01)" and step 1.4 – "Establish SaaS governance model and adoption principles", accordingly. Although the least rated task in step 1 was the "SaaS application suitability" scoring the lowest weighted average of 3.65. It should be clear from the corresponding figure that these individual tasks were perceived to have different levels of importance (e.g. absolutely, very, slightly etc.). For instance, while the lesser minority (1%) of respondents found step 1.1 to be not at all important, a greater majority (51%) rated it the highest. The need for requesting for all this diverse information from respondents lies in the fact that from a vendor lock-in risk management perspective, a lock-in situation with a high probability of occurrence may not have a high impact (i.e. hindrance or obstruction) on the organisation migrating to the cloud, and vice versa. As a typical example, a provider going out of business is lock-in risk event that often has high impact but low probability of occurrence. Therefore, while evaluating the importance of a lock-in risk event (as in step 1.); it is necessary and crucial to consider the following tasks and their corresponding activities, namely step 1.3 – "SaaS application suitability test (3.65)" and also step 1.2 – "Requirement analysis (3.79)". For a detailed analysis in this aspect, please refer to *Section 6.1*.

To evaluate the general *appropriateness* of each task identified within step 1, the overall perception gathered from respondents in **Figure 5.22** show that the corresponding tasks and supporting activities were all considered appropriate for decision step 1. Similar to the result obtained from **Figure 5.21**, herein step 1.5 – "SaaS risk assesment and mitigation " scored the highest weighted mean value of 4.31 out of 5, while step 1.3 – "SaaS application suitability" scored the lowest rating of 3.56. Moreover, the need to establish a governace and adoption principles (i.e. step 1.4) for SaaS within existing enterprise organisation is regarded a high priority (3.90) when compared to the task of defining organisational context (3.88) for the migration.

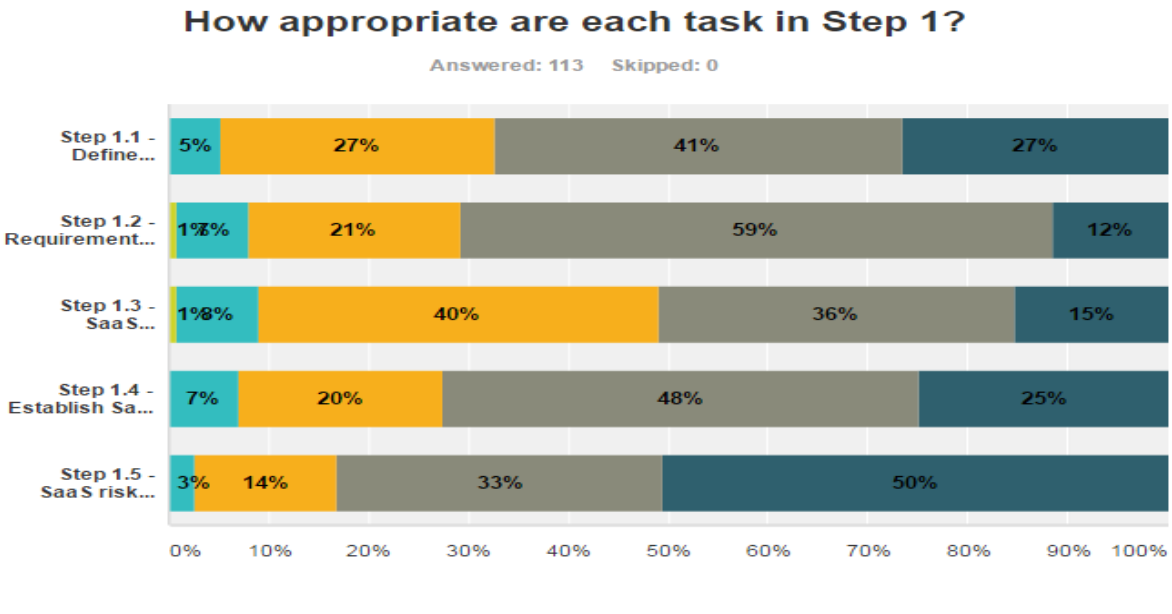


	0 (Not at all important) (1)	1 (2)	2 (3)	3 (4)	4 (Absolutely important) (5)	Total	Weighted Average
Step 1.1 - Define organisational context	1% 1	5% 6	14% 16	51% 58	28% 32	113	4.01
Step 1.2 - Requirement analysis	0% 0	9% 10	21% 24	52% 59	18% 20	113	3.79
Step 1.3 - SaaS application suitability	0% 0	6% 7	35% 39	47% 53	12% 14	113	3.65
Step 1.4 - Establish SaaS governance model and adoption principles	0% 0	10% 11	18% 20	44% 50	28% 32	113	3.91
Step 1.5 - SaaS risk assessment and mitigation	0% 0	5% 6	14% 16	32% 36	49% 55	113	4.24

Figure 5.21-Importance of Tasks within Step 1

As shown in this result, if IT governance and SaaS adoption principles by the cloud service provider is a significant concern for the cloud service consumer, then cloud service customers are advised to establish (*refer to* **Figure 5.7**) if a cloud service provider complies with one or more of these (e.g. COBIT, ISO 38500, ITIL, HIPAA, PCI-DSS, etc.) governance and management standards. While these standards are not specific to cloud computing, however they are sufficiently general enough to be applied to the govenrance of cloud computing. Moreover as highlighted earlier, SaaS risk assessment and mitigation (i.e. step 1.5) was identified by IT proffesionals as the most *important* (49%) and *appropiate* (59%) task in step 1. To evaluate the general usefulness of the responses received, this survey result signifies that, prior to migrating to cloud SaaS environments, organisations need to implement proper risk assessment measures to proactively secure their business-critical and non-critical applications and data from external and internal lock-in challenges and security threats throughout their entire life cycle, from design to implementation to production *(refer to Section 5.4.1).* Clearly defined governance policies, standards, security policies and processes are critical to ensure the migrated application and data is enabling the business rather than introducing additional lock-in risks.

In particular, we can see from **Figure 5.22** that there were a lot of diverse responses, with the exact number of responses for each identified task (i.e. answer option) within step 1. The minimum and maximum columns in the figure show the highest and lowest number answer option that received at least one response. Therefore, a mean of 4.31 (i.e. in the case of step 1.5) shows that overall respondents came in somewhere between "very *appropriate*" and "absolutely *appropriate*". However, it could be observed that there is some nuance to the mean and median numbers in the figure below. Statistically, what this shows is that the median of 5 (i.e. higher than 4.31) further suggests that the results for assessing the propriety of step 1.5 are about evenly distributed between (very and absolutely *appropriate*) positive responses. Overall, comparison of the identified tasks (within step1) based on descriptive statistics computation furthermore shows that the difference between the largest and smallest wieighted mean values (i.e. 4.31 – 3.56) for all rated tasks in step 1 is less than the least standard deviation (i.e. 0.79) for a single task. What this implies is that the largest standard deviation from the sample means (i.e. 0.87) is less than twice the smallest (2 * 0.79 = 1.5) which further illustrates that the survey data is reasonably normal. As a result, the tasks within step 1 are inferred to be *appropriate* and the following evaluation results of the novel decision framework can be considered reasonable. Note, the decriptive analysis and interpretation of data presented above applies to all subsequent sections of this evaluation report (for readability and clarity purpose).



	0 (Not at all appropriate) (1)	1 (2)	2 (3)	3 (4)	4 (Absolutely appropriate) (5)	Total	Weighted Average
Step 1.1 - Define organisational context	0% 0	5% 6	27% 31	41% 46	27% 30	113	3.88
Step 1.2 - Requirement analysis	1% 1	7% 8	21% 24	59% 67	12% 13	113	3.73
Step 1.3 - SaaS application suitability	1% 1	8% 9	40% 45	36% 40	15% 17	112	3.56
Step 1.4 - Establish SaaS governance model and adoption principles	0% 0	7% 8	20% 23	48% 54	25% 28	113	3.90
Step 1.5 - SaaS risk assessment and mitigation	0% 0	3% 3	14% 16	33% 37	50% 57	113	4.31

Basic Statistics

	Minimum	Maximum	Median	Mean	Standard Deviation
Step 1.1 - Define organisational context	2.00	5.00	4.00	3.88	0.86
Step 1.2 - Requirement analysis	1.00	5.00	4.00	3.73	0.79
Step 1.3 - SaaS application suitability	1.00	5.00	4.00	3.56	0.87
Step 1.4 - Establish SaaS governance model and adoption principles	2.00	5.00	4.00	3.90	0.85
Step 1.5 - SaaS risk assessment and mitigation	2.00	5.00	5.00	4.31	0.81

Figure 5.22- Appropriateness of Tasks in Step 1

- *Tasks within the Vendor Evaluation and Selection* ***Step 2***

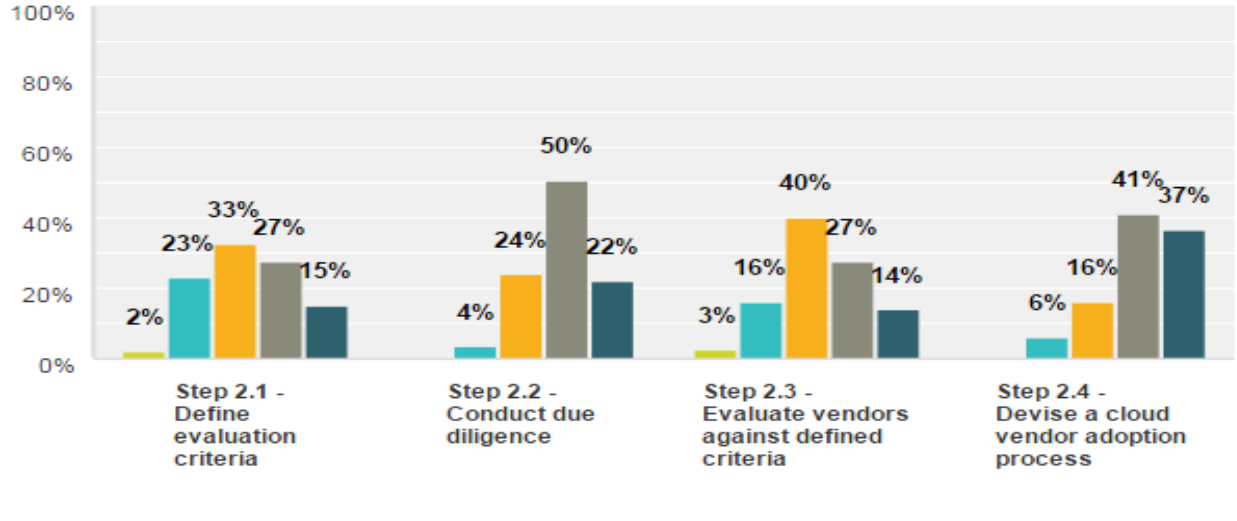
As depicted in the figure below, participants were asked to rate the *importance* of the tasks identified in step 2 – "Vendor evaluation and selection". **Figure 5.23** provides the evaluation results for this decision step and supporting activities. Generally, all tasks within this step are rated as important, with the minimum weighted average value of 3.31 (i.e. moderately important) or higher. In spite of the fact that step 2.1 (i.e. define evaluation criteria task) and step 2.3 (evaluate vendors against defined criteria) were the least rated on the scale of *importance*, this also shows that IT decision-makers and cloud architects are less interested in performing these tasks. Nonetheless, organisations should be very cautious when evaluating vendors against specific criteria or making decision towards the selection of cloud vendors (*refer to Section 5.4.2*) – considering the potential difficulties for changing either during or at the end of the contract. This is crucial because organisations can suffer very substantial financial loss if they did not make strategically correct vendor selection decision at the very beginning. However, the greater majority of respondents place more value on either devising a vendor adoption technique (4.08) and/or conducting proper due diligence (3.91). Therefore, a mean of 4.08 (i.e. in the case of step 2.4) overall shows the significant number of respondents who perceived this task as critical came in somewhere between "very *important*" and "absolutely *important*". In the case of step 2.2, it could be observed also that some nuance do exist between the mean and median numbers for instance. The difference between the mean and median values in step 2.2 (i.e. 0.09 higher than 3.91) shows that even though about half of the number (50%) of respondents said the conduct due diligence task was very *important*, there were more respondents who perceived it to be absolutely *important* (22%) than respondents who thought it was slightly *important* (4%). Moreover, the largest standard deviation (1.04) for all answer options in this step is less than twice the smallest (2 * 0.77 = 1.54) which shows normality of data.

With respect to evaluating the general *appropriateness* of each task identified in step 2, the overall results gathered from IT practtioners in **Figure 6.18** show that the corresponding tasks and supporting activities were all considered appropriate, while the average rating for individual task is actually ranked higher. The tasks in this step scored an average of 3.7 out of 5. However, similar to the results computed above for *importance*, herein, step 2.2 –"conduct due dilligence (4.04)" and step 2.4 – "devise a cloud vendor adoption process (4.04)" were rated equally by participants as very and absolutely *appropriate*. This further shed some light on the relevance of each of these tasks regarding vendor evaluation. Another view of vendor comparison is shown in research by (Sarapali and Pingali, 2011) which refers to a vendor characterisation excel-tool provided by Info-tech research that considers attributes like available features, affordability, usability, vendor viability, and support quality to point out an appropriate cloud vendor. But, those outlined attributes indicate to cloud service consumers that a vendor comparison in this case incorporates hard technical and functional

facts considered by tasks like cost analysis etc. In terms of the novel 6-step decision framework proposed in this PhD study, this decision step 2 is expected to evaluate a cloud vendor to the approach discussed in *Section 3.8.1* (*or see* **Figure 5.6** *for illustration*), which is deemed to be more suitable for a subjective cloud service selection and discrete vendor evaluation (Gudenkauf et al. 2013) rather than the latter approach that mixes up aspects already considered by other parts of the proposed decision framework. The least rated task in this step was step 1.1 – "defining evaluation criteria (3.39)" and step 2.3 – "evaluate vendors against defined criteria (3.31)". Although it could be seen in the case of step 2.3, that while a considerable amount of IT practitioners (13%) rated this task as absolutely *appropriate*, a lesser minority considered it to be not at all *appropriate*. Notwithstanding, a mean of 3.31 suggest that overall IT practitioners and decision-makers still considered the activities in step 2.3 to be moderately appropriate during a vendor evaluation and selection process.

Please rate the importance of each of the following task in Step 2 (i.e. Vendor Evaluation and Selection).

Answered: 113 Skipped: 0

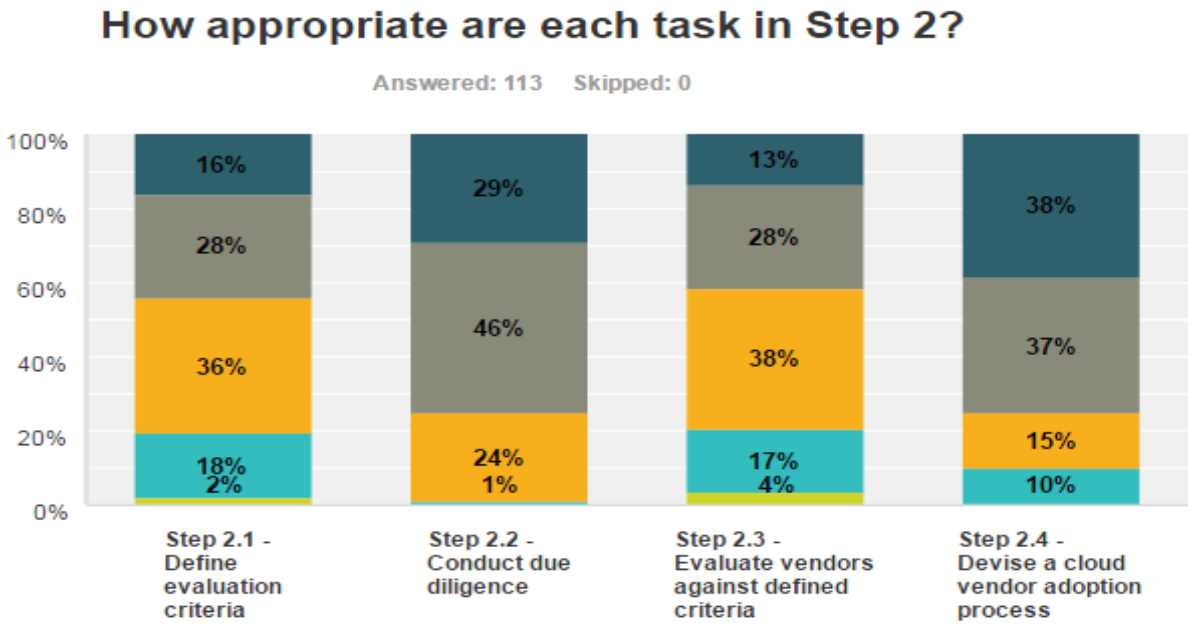


	0 (Not at all important) (1)	1 (2)	2 (3)	3 (4)	4 (Absolutely important) (5)	Total	Weighted Average
Step 2.1 - Define evaluation criteria	2% 2	23% 26	33% 37	27% 31	15% 17	113	3.31
Step 2.2 - Conduct due diligence	0% 0	4% 4	24% 27	50% 57	22% 25	113	3.91
Step 2.3 - Evaluate vendors against defined criteria	3% 3	16% 18	40% 45	27% 31	14% 16	113	3.35
Step 2.4 - Devise a cloud vendor adoption process	0% 0	6% 7	16% 18	41% 46	37% 41	112	4.08

Basic Statistics

	Minimum	Maximum	Median	Mean	Standard Deviation
Step 2.1 - Define evaluation criteria	1.00	5.00	3.00	3.31	1.04
Step 2.2 - Conduct due diligence	2.00	5.00	4.00	3.91	0.77
Step 2.3 - Evaluate vendors against defined criteria	1.00	5.00	3.00	3.35	0.99
Step 2.4 - Devise a cloud vendor adoption process	2.00	5.00	4.00	4.08	0.88

Figure 5.23-Importance of Tasks within Step 2



	0 (Not at all appropriate) (1)	1 (2)	2 (3)	3 (4)	4 (Absolutely appropriate) (5)	Total	Weighted Average
Step 2.1 - Define evaluation criteria	2% 2	18% 20	36% 41	28% 32	16% 18	113	3.39
Step 2.2 - Conduct due diligence	0% 0	1% 1	24% 27	46% 52	29% 33	113	4.04
Step 2.3 - Evaluate vendors against defined criteria	4% 4	17% 19	38% 43	28% 32	13% 15	113	3.31
Step 2.4 - Devise a cloud vendor adoption process	0% 0	10% 11	15% 17	37% 41	38% 43	112	4.04

Basic Statistics

	Minimum	Maximum	Median	Mean	Standard Deviation
Step 2.1 - Define evaluation criteria	1.00	5.00	3.00	3.39	1.01
Step 2.2 - Conduct due diligence	2.00	5.00	4.00	4.04	0.75
Step 2.3 - Evaluate vendors against defined criteria	1.00	5.00	3.00	3.31	1.01
Step 2.4 - Devise a cloud vendor adoption process	2.00	5.00	4.00	4.04	0.96

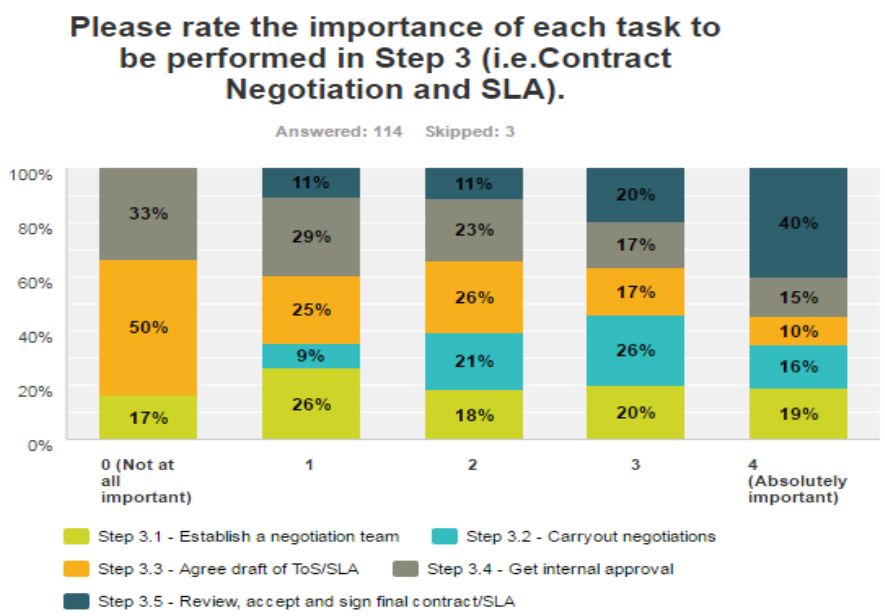
Figure 5.24- Appropriateness of Tasks within Step 2

5.10.2 Phase 2 – Contract and Service Provision

- Tasks within the Contract Negotiation and SLA Step 3

Figure 5.25 and **Figure 5.26** provides the evaluation results for the tasks that are performed in the contract negotiation and SLA step. As depicted in **Figure 5.25**, step 3.5 – "review, accept and sign final contract/SLA" was rated the highest (4.12) on the scale of importance, followed by step 3.2 – "carryout negotiations (3.76)", and step 3.1 – "establish negotiation team (3.57)". The least task in average weightings evaluated by participants was step 3 (3.40) and step 3.3 (3.32). In a nutshell, what this result synopsizes is that IT practitioners and decision-makers prioritise the tasks and supporting activities within step 3.5, hence seeing it as the most *important* amongst others. Quite simply, this finding is not unusual but very intriguing seeing as the general basis on which cloud providers and cloud customers enter into a binding relationship falls into two clear categories – depending on whether the provider is offering a paid service or a free one. However, while some free services may impose non-monetary costs on the customer, such as imposition of licence terms that allow the provider to re-use the customer's data for its own purpose. Likewise, paid services themselves fall into a spectrum between those entered into on the basis of the standard-form contract of the provider and those where the contract terms are fully negotiated, depending on the relative barraging power of provider and customer (*refer to Section 5.4.3*). Furthermore, some service may offer a free trial period conditional on the customer giving payment details, which then converts into a paid contract. Such complicated distinctions further magnify the relevance of step 3.5. However, in order to meet the contractual requests of cloud service customers by their providers, firstly, it is also critical to understand the implications of any legislation or regulation in effect that is relevant to application and/or data migration; and secondly, many individual capabilities of the cloud service have to exist and the related obligations and activities should be mutually agreed upon (i.e. step 3.4), and captured in a draft cloud SLA (as in step 3.3) or corresponding contractual agreement (i.e. Step 3.2) set up between both parties. While the task in step 3.1 was weighted at 3.57 out of 5 on average, and with a corresponding median value of 4 suggests why most respondents considered it to be moderately *important*. It is also important, in general, to consider conformance issues when carrying out negotiations with potential cloud providers because conformance has proven to be problematic since cloud service might be conformant at certain levels (e.g. technical and semantic levels), while still non-compliant at others (e.g. process and legal levels). Therefore, the issue of conformance including support for validation and verification of the technologies involved in securing the portability and interoperability between cloud-based SaaS solutions and platforms should be addressed when procuring a cloud service. Additionally, as depicted in **Figure 5.26**, step 3.2 (3.57) as the second most *appropriate* task rated by IT practitioners concurs on the need to negotiate the cloud SLA to cover obligations of the cloud service provider in terms of interoperability, portability, exit clause, data

protection and security which could all be supported by defining values for standardised metrics in those aspects.



	Step 3.1 - Establish a negotiation team	Step 3.2 - Carryout negotiations	Step 3.3 - Agree draft of ToS/SLA	Step 3.4 - Get internal approval	Step 3.5 - Review, accept and sign final contract/SLA	Total	Weighted Average
0 (Not at all important) (1)	17% 1	0% 0	50% 3	33% 2	0% 0	6	1.00
1 (2)	26% 20	9% 7	25% 19	29% 22	11% 8	76	2.00
2 (3)	18% 28	21% 32	26% 40	23% 35	11% 17	152	3.00
3 (4)	20% 43	26% 56	17% 37	17% 37	20% 42	215	4.00
4 (Absolutely important) (5)	19% 22	16% 19	10% 12	15% 17	40% 47	117	5.00

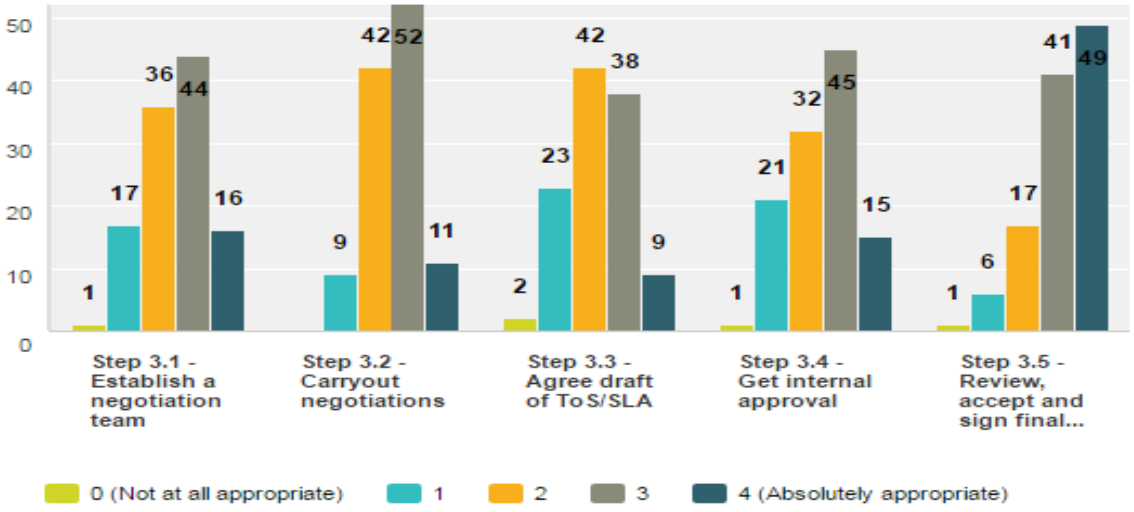
Basic Statistics

	Minimum	Maximum	Median	Mean	Standard Deviation
Step 3.1 - Establish a negotiation team	1.00	5.00	4.00	3.57	1.02
Step 3.2 - Carryout negotiations	2.00	5.00	4.00	3.76	0.80
Step 3.3 - Agree draft of ToS/SLA	1.00	5.00	3.00	3.32	0.97
Step 3.4 - Get internal approval	1.00	5.00	3.00	3.40	1.02
Step 3.5 - Review, accept and sign final contract/SLA	2.00	5.00	4.00	4.12	0.91

Figure 5.25-Task Evaluation in Step 3 – Importance

How appropriate are each task in Step 3?

Answered: 114 Skipped: 3



	0 (Not at all appropriate) (1)	1 (2)	2 (3)	3 (4)	4 (Absolutely appropriate) (5)	Total	Weighted Average
Step 3.1 - Establish a negotiation team	0.88% 1	14.91% 17	31.58% 36	38.60% 44	14.04% 16	114	3.50
Step 3.2 - Carryout negotiations	0.00% 0	7.89% 9	36.84% 42	45.61% 52	9.65% 11	114	3.57
Step 3.3 - Agree draft of ToS/SLA	1.75% 2	20.18% 23	36.84% 42	33.33% 38	7.89% 9	114	3.25
Step 3.4 - Get internal approval	0.88% 1	18.42% 21	28.07% 32	39.47% 45	13.16% 15	114	3.46
Step 3.5 - Review, accept and sign final contract/SLA	0.88% 1	5.26% 6	14.91% 17	35.96% 41	42.98% 49	114	4.15

Basic Statistics

	Minimum	Maximum	Median	Mean	Standard Deviation
Step 3.1 - Establish a negotiation team	1.00	5.00	4.00	3.50	0.94
Step 3.2 - Carryout negotiations	2.00	5.00	4.00	3.57	0.77
Step 3.3 - Agree draft of ToS/SLA	1.00	5.00	3.00	3.25	0.93
Step 3.4 - Get internal approval	1.00	5.00	4.00	3.46	0.97
Step 3.5 - Review, accept and sign final contract/SLA	1.00	5.00	4.00	4.15	0.92

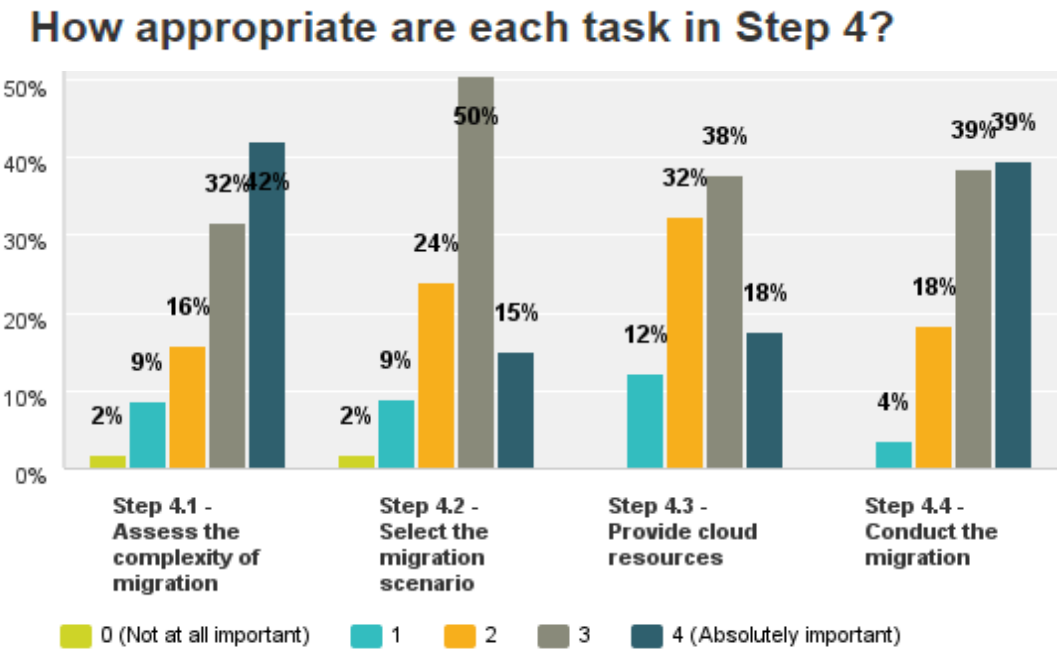
Figure 5.26-Task Evaluation in Step 3 – Appropriateness

- *Tasks within the Design and Execute the Migration* ***Step 4***

One of the key objectives of the evaluation survey questionnaire was to examine the *importance* and *appropriateness* of the tasks and supporting activities within each individual step of the novel decision framework. This framework has been developed to encompass cross-cutting challenges that affect cloud migration decision making at the strategic level, but with a specific focus on the tactical and prescriptive strategies to avoid the vendor lock-in problem at SaaS layer (*refer to Section 6.4*). **Figure 5.27** shows the tasks for step 4 as being evaluated by IT practitioners and enterprise decision makers. The rating for each individual task within this step was scored from 0 to 4, with zero indicating not at all *important* (or *appropriate*) and four absolutely important (or *appropriate*).

Figure(s) **5.27** and **Figure 5.28** depicts the findings in step 4, and shows an overall higher rating in both task *importance* and *appropriateness* of the activities performed when making informed decisions to migrate application/data to cloud computing. Every task scored more than 3 out of 5, indicating that all identified tasks within this step were regarded as either moderately *important* (i.e. moderately *appropriate* as in **Figure 5.27**) or very *important* (i.e. very *appropriate* as in **Figure 5.28**). Arguably, the results show that IT practitioners and cloud migration specialists are in agreement that the tasks and supporting activities performed within the design and execute the migration step have a significant impact on cloud computing adoption decisions, as well as technical strategies to avoid vendor lock-in. More importantly, the result in **Figure 5.27** shows the top rated task as step 4.4 (4.14) when compared to the weighted score for step 4.1 (4.04). However, in step 4.1 a mean value of 4.04 and median of 4.00 shows that while 2% of the average respondents rated this task as not at all important, the significant (42%) majority considered it absolutely important. The standard deviation (or SD) of 1.04 (i.e. 0.2 > than the lowest SD = 0.84), signifies a dispersion in the number of responses for each answer option in step 4.1. However, step 4.4 and step 4.1 in both figures were scored the highest, while amongst the same figures the least rated task in this step was seen to be step 4.2 – "select the migration scenario". Although when comparing the results (i.e. step 4.1 vs. step 4.4 weighted values), it is clear across both axis that participants consider the tasks in step 4 to be more *appropriate* than *important*. See screen dump attached below for additional comments made by IT practitioners who felt there were some missing attributes from the tasks performed in step 4.

#	Is there any important attribute missing from the tasks in Step 4 above? Other (please specify here):
1	Note:The Select migration scenario - i.e. Step 4.2 in some cases may have already been defined in Step 1, hence why it was rated as not all important. Notwithstanding, the Step 4.2 could be applicable to different organisations as per the migration project at hand.
2	None
3	Ps: not always is it possible to negotiate a standard contract - although experience shows the power of negotiation lies within the service being purchased and the vendor capability to meet agreed SLA. Even when such negotiations are reached there may also be costs associated with the negotiations



	0 (Not at all important) (1)	1 (2)	2 (3)	3 (4)	4 (Absolutely important) (5)	Total	Weighted Average
Step 4.1 - Assess the complexity of migration	**2%** 2	**9%** 10	**16%** 18	**32%** 36	**42%** 48	114	4.04
Step 4.2 - Select the migration scenario	**2%** 2	**9%** 10	**24%** 27	**50%** 57	**15%** 17	113	3.68
Step 4.3 - Provide cloud resources	**0%** 0	**12%** 14	**32%** 37	**38%** 43	**18%** 20	114	3.61
Step 4.4 - Conduct the migration	**0%** 0	**4%** 4	**18%** 21	**39%** 44	**39%** 45	114	4.14

Basic Statistics

	Minimum	Maximum	Median	Mean	Standard Deviation
Step 4.1 - Assess the complexity of migration	1.00	5.00	4.00	4.04	1.04
Step 4.2 - Select the migration scenario	1.00	5.00	4.00	3.68	0.90
Step 4.3 - Provide cloud resources	2.00	5.00	4.00	3.61	0.91
Step 4.4 - Conduct the migration	2.00	5.00	4.00	4.14	0.84

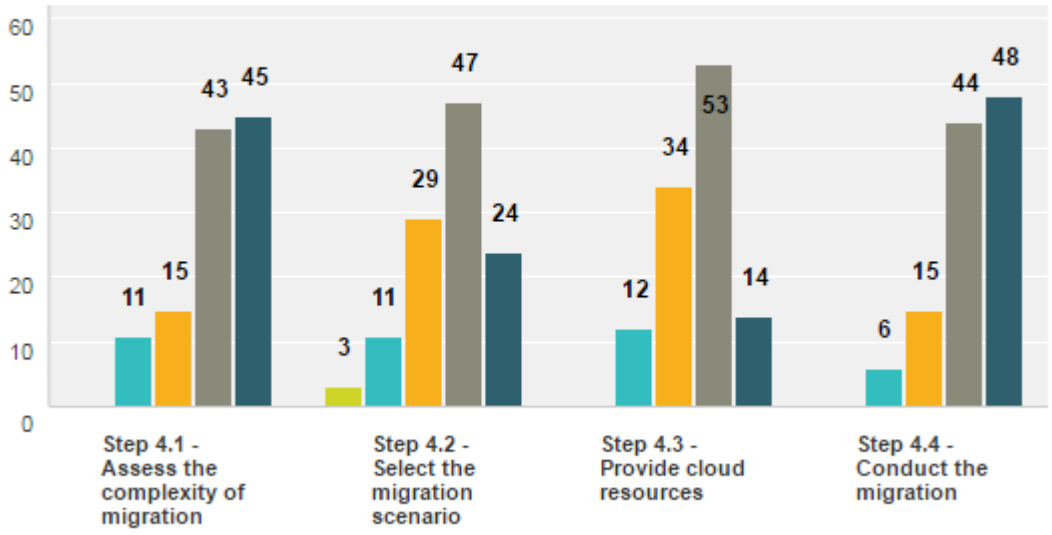
Figure 5.27-Task Evaluation in Step 4 – Importance

Therefore, on the scale of priority or propriety (*see* **Figure 5.28**), the significance of the step 4.1 (4.19) cannot be over emphasised or underestimated as has already been confirmed by result evaluation from IT practitioners who participated in the study. Assessing the complexity of migration in cloud environment is a crucial service delivery task when planning to avoid potential risks of vendor lock-in. In fact, the task is appropriate simply because to logically and physically transition (i.e. move) computational aspects of applications and data over the cloud (or across cloud providers and on-premise IT environments) creates a series of technical (*see Section 4.5.3*), legal (*see Section 4.5.10*), and business-related (*see Section(s) 4.5.5–4.5.9*) challenges of vendor lock-in (*refer to Section 3*) for all types of migration (*see Section 2.9*). Moreover, these aspects of vendor lock-in are further complicated by QoS dimensions like service availability and reliability which thus becomes very important for the operation of the cloud-migrated or replaced SaaS application.

QoS levels must be evaluated when conducting an assessment for migration complexity (as in step 4.1), as it entails two key factors worth considering, namely: 1) performance variability of the cloud provider, and; 2) the network latency between the cloud service consumers and the service (i.e. application and the service in the case of Type I and Type II migrations, and the application consumers and the application itself for Type III and Type IV migrations). Further, another factor worth considering, when assessing the migration complexity, is the isolation aspect of multi-tenancy and its implications on QoS characteristics of cloud-enabled SaaS application. This challenge is further complicated due to the closed nature of the cloud, which provides limited visibility to the underlying subsystems and consequently makes the evaluation of isolation, from a cloud architects perspective, a difficult and elusive task to accomplish. In fact, this issue is a recognised problem, and thus a subject-topic of ongoing research initiatives, for example (Alexandrov et al. 2012; Joukov et al. 2011). Furthermore, being that cloud SaaS services move the responsibility and effort for enabling multi-tenancy to the service provider, therefore a different degree of adaptation may be required (and assessed in step 4 via step 4.1, accordingly) to application depending on the type of migration (as in step 4.2) and cloud service model. In summary, to confer from the survey evaluation result for decision step 4 (*see* **Figure 5.28**), overall findings show that participants recognise the relevance of each identified task within this decision step – although priority of discussion presented herein is placed on the top-rated tasks (i.e. step 4.1 and 4.4). Therefore, as a recommendation, author suggests that when discussing multi-tenancy requirements (as in step 4.1) of a cloud-based SaaS application within an enterprise context, the views of involved parties (i.e. customer and provider/vendor) should be considered, and more importantly for the customers of the migrated SaaS application, they need to ensure they are provided with customization capabilities.

How appropriate are each task in Step 4?

Answered: 114 Skipped: 3



	0 (Not at all appropriate) (1)	1 (2)	2 (3)	3 (4)	4 (Absolutely appropriate) (5)	Total	Weighted Average
Step 4.1 - Assess the complexity of migration	0.00% 0	9.65% 11	13.16% 15	37.72% 43	39.47% 45	114	4.07
Step 4.2 - Select the migration scenario	2.63% 3	9.65% 11	25.44% 29	41.23% 47	21.05% 24	114	3.68
Step 4.3 - Provide cloud resources	0.00% 0	10.62% 12	30.09% 34	46.90% 53	12.39% 14	113	3.61
Step 4.4 - Conduct the migration	0.00% 0	5.31% 6	13.27% 15	38.94% 44	42.48% 48	113	4.19

Basic Statistics

	Minimum	Maximum	Median	Mean	Standard Deviation
Step 4.1 - Assess the complexity of migration	2.00	5.00	4.00	4.07	0.95
Step 4.2 - Select the migration scenario	1.00	5.00	4.00	3.68	0.99
Step 4.3 - Provide cloud resources	2.00	5.00	4.00	3.61	0.84
Step 4.4 - Conduct the migration	2.00	5.00	4.00	4.19	0.86

Figure 5.28-Task Evaluation in Step 4 – Appropriateness

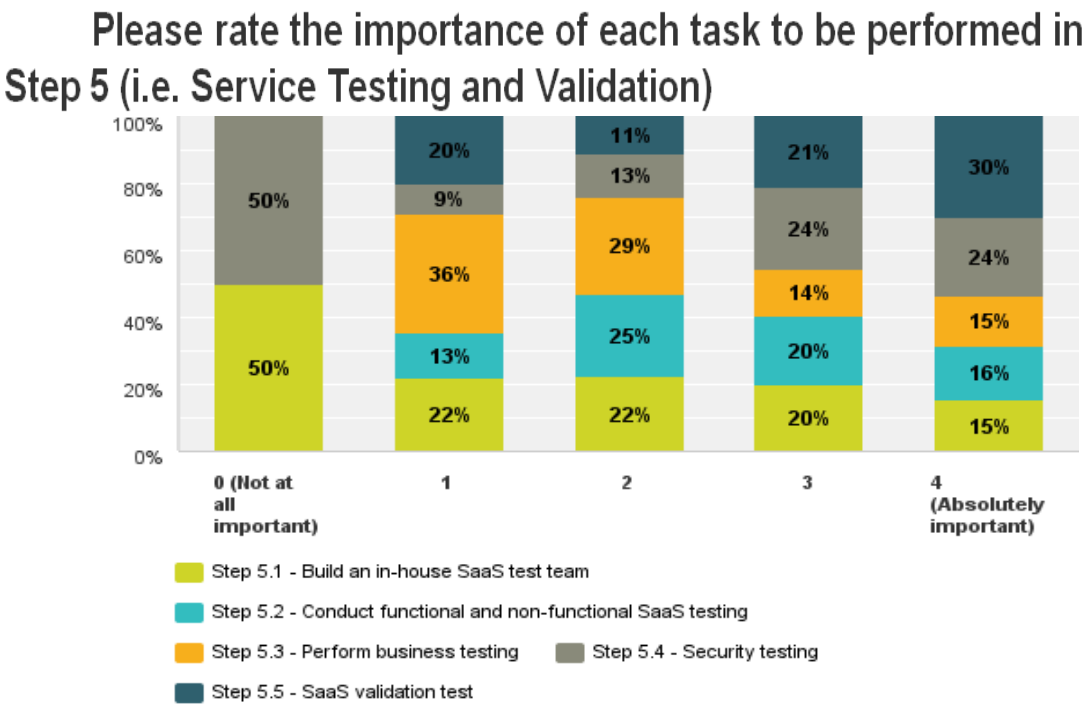
5.10.3 Phase 3 – Service Validation and Management

- *Tasks within the Service Testing and Validation* ***Step 5***

Participants were asked to rate the *importance* (see **Figure 5.29**) and *appropriateness* (*see* **Figure 5.30**) of each individual task identified in step 5 – "service testing and validation", with 4 being absolutely *important* (or absolutely *appropriate*) and 0 being not at all *important* (or not *appropriate*). There are five main tasks to be performed in step 5, as shown in the figures below. With an average weighted rating of 3.76 out of 5, the results show the respondents level of agreement with the tasks identified within step 5. In this step, the least rated tasks were step 5.3 – "perform business testing (3.48)" and step 5.1 – "build an in-house SaaS test team (3.63)". However, on average, IT practitioners placed more *importance* on step 5.5 (4.02), step 5.4 (3.95), and step 5.2 (3.73). Therefore, while the task labelled "SaaS validation test" was rated amongst others the highest in terms of *importance*, on the contrary, it could be seen in **Figure 5.30** that the task labelled "security testing – step 5.4 (4.05) was rated the highest on the scale *appropriateness*. When comparing both results (i.e. *importance* vs. *appropriate*) based on their descriptive statistical values, alternatively it is quite clear that the tasks in step 5.3 (3.48) and step 5.1 (3.57) were the least rated overall for step 5.

Taking the former case for instance, the mean value of 3.48 shown in **Figure 5.29**, suggests that the overall responses from IT practitioners who rated step 5.3 came in somewhere between moderately *important* and very *important*. Although further data analysis in these aspects suggests some nuance exist between the mean and median values on both scales (i.e. appropriateness and importance). A median of 3.00 (less than the 3.48 mean) shows that answers were oddly distributed between negative (slightly *important*) and positive (moderately *important*) responses. This difference between the mean and the median shows that even though about 29% of IT practitioners and decision makers regarded the task in step 5.3 as very *important*, there were more respondents who considered it to be slightly *important* than respondents who thought it was moderately *important*.

Regarding the latter case (i.e. *appropriate*), the mean value of 3.57 shown in **Figure 5.10** suggests that overall respondents in step 5.1 came in somewhere between moderately *appropriate* and very *appropriate*. However, there is some nuance to the numbers also when it comes to comparing the mean and median. The median represents the answer option in the middle of all responses which indicates there are an equal number of responses above and below the answer option. Thus, a median of 4 (higher than the 3.57 mean) shows that the responses are distributed around very *appropriate* responses. The difference between the mean and median, as in the paragraph above, shows in this case that although equal number (38%) of practitioners and decision-makers said this task (i.e. step 5.1) was moderately and very appropriate, there were more respondents who rated it absolutely appropriate than respondents who rated it slightly appropriate.

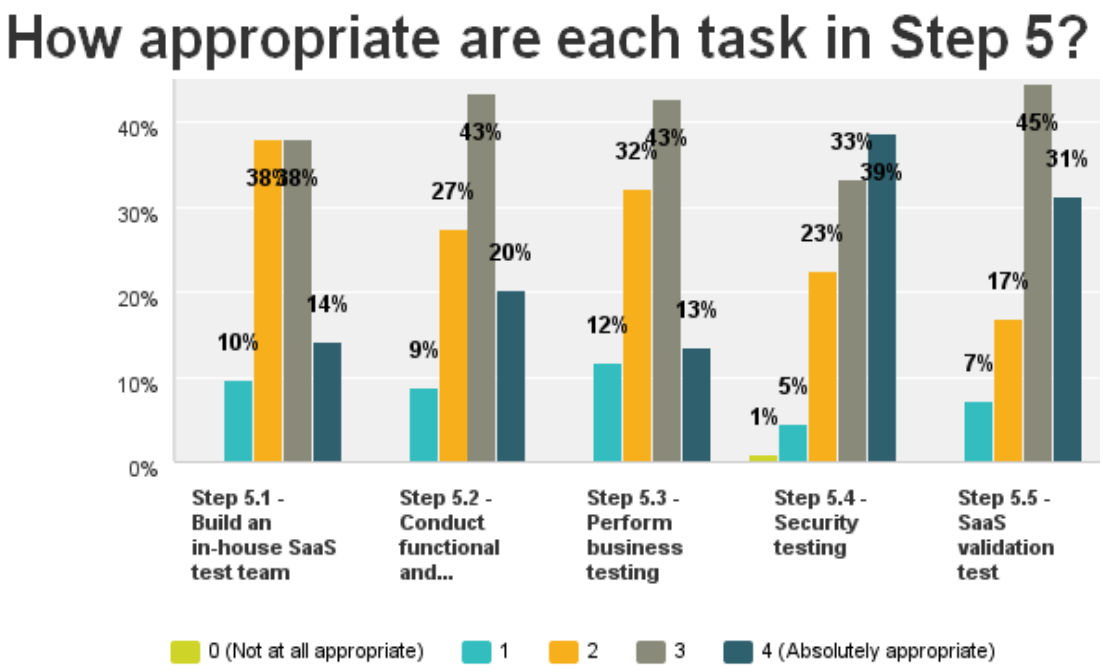


	Step 5.1 - Build an in-house SaaS test team	Step 5.2 - Conduct functional and non-functional SaaS testing	Step 5.3 - Perform business testing	Step 5.4 - Security testing	Step 5.5 - SaaS validation test	Total	Weighted Average
0 (Not at all important) (1)	**50%** 2	**0%** 0	**0%** 0	**50%** 2	**0%** 0	4	1.00
1 (2)	**22%** 10	**13%** 6	**36%** 16	**9%** 4	**20%** 9	45	2.00
2 (3)	**22%** 35	**25%** 39	**29%** 45	**13%** 21	**11%** 17	157	3.00
3 (4)	**20%** 47	**20%** 48	**14%** 34	**24%** 57	**21%** 50	236	4.00
4 (Absolutely important) (5)	**15%** 19	**16%** 20	**15%** 18	**24%** 29	**30%** 37	123	5.00

Basic Statistics

	Minimum	Maximum	Median	Mean	Standard Deviation
Step 5.1 - Build an in-house SaaS test team	1.00	5.00	4.00	3.63	0.92
Step 5.2 - Conduct functional and non-functional SaaS testing	2.00	5.00	4.00	3.73	0.81
Step 5.3 - Perform business testing	2.00	5.00	3.00	3.48	0.92
Step 5.4 - Security testing	1.00	5.00	4.00	3.95	0.86
Step 5.5 - SaaS validation test	2.00	5.00	4.00	4.02	0.89

Figure 5.29-Task Evaluation in Step 5 – Importance



	0 (Not at all appropriate) (1)	1 (2)	2 (3)	3 (4)	4 (Absolutely appropriate) (5)	Total	Weighted Average
Step 5.1 - Build an in-house SaaS test team	0% 0	10% 11	38% 43	38% 43	14% 16	113	3.57
Step 5.2 - Conduct functional and non-functional SaaS testing	0% 0	9% 10	27% 31	43% 49	20% 23	113	3.75
Step 5.3 - Perform business testing	0% 0	12% 13	32% 36	43% 48	13% 15	112	3.58
Step 5.4 - Security testing	1% 1	5% 5	23% 25	33% 37	39% 43	111	4.05
Step 5.5 - SaaS validation test	0% 0	7% 8	17% 19	45% 50	31% 35	112	4.00

Basic Statistics

	Minimum	Maximum	Median	Mean	Standard Deviation
Step 5.1 - Build an in-house SaaS test team	2.00	5.00	4.00	3.57	0.85
Step 5.2 - Conduct functional and non-functional SaaS testing	2.00	5.00	4.00	3.75	0.88
Step 5.3 - Perform business testing	2.00	5.00	4.00	3.58	0.86
Step 5.4 - Security testing	1.00	5.00	4.00	4.05	0.93
Step 5.5 - SaaS validation test	2.00	5.00	4.00	4.00	0.88

Figure 5.30-Task Evaluation in Step 5 – Appropriateness

- *Tasks within the Service Operation and Optimization* ***Step 6***

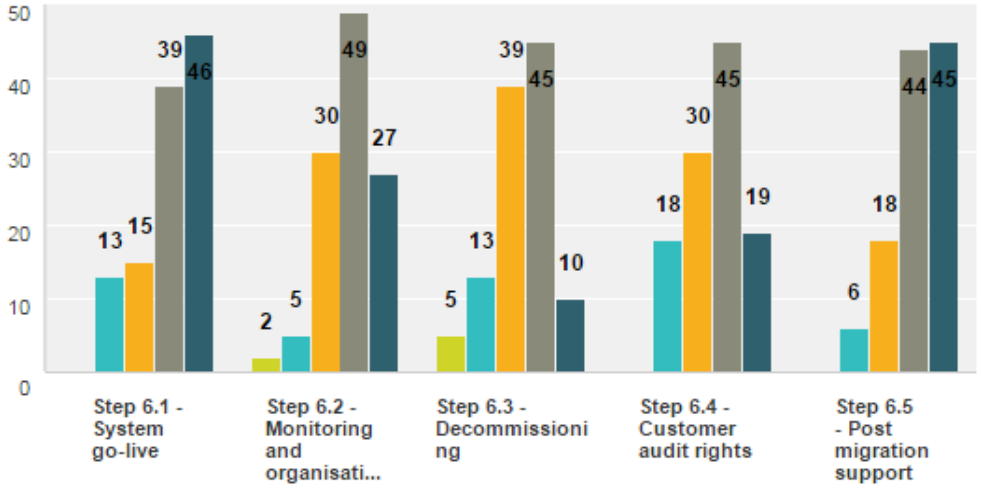
Last but certainly not least, "service operation and optimization" is the final step in this novel 6-step decision framework to avoid vendor lock-in challenges in cloud SaaS migration. The tasks within this step were evaluated by IT practitioners and enterprise decision-makers to identify the most important (see **Figure 5.31**) and most appropriate (see **Figure 5.32**). As shown in both figures, step 6.5 and step 6.1 were rated the highest in terms of *importance* (i.e. 4.13; 4.04) and *appropriate* (i.e. 4.27; 4.02), respectively. Likewise, across both figures also the tasks labelled "decommissioning – step 6.3 (3.38; 3.29)" and "customer audit right – step 6.4 (3.58; 3.66)" respectively, scored the lowest ratings on average in terms of IT practitioners views of their *importance* and *appropriateness* for dealing with the vendor lock-in problem at service operation and optimization phase.

Regardless of the individual weighted average values, all tasks within step 6 scored average ratings of 3.79 (*importance*) and 3.59 (*appropriate*) out of 5. In a nutshell, this result perhaps suggests the tasks evaluated within this decision step (6) were all rated highly, by IT practitioners and decision-makers, for their *importance* when compared to its *propriety*. Nevertheless, each task and corresponding activity performed in this step is crucial to avoiding the vendor lock-in problem at operational levels, and at post migration phase (*refer to Section 5.4.6*). Taking step 6.5 for instance, a key requirement for this task is a well-defined and documented exit process or roll back plan. The significance of the activities to be performed in this step, for example, is well recognised as has already been highlighted in a recent ISO (2015) research report which commends that, "the termination of use and the exit process for cloud computing are subjects that ned to be addressed, as such new research proposals and agendas should be initiated to address gaps in this knowledge area". In this regard, author recommends customers to negotiate directly with their cloud service providers (as in step 3.2) to ensure appropriate exit process provisions and assurances (from vendor lock-in) are included and adequately documented in their cloud SLA (*refer to Section(s) 4.5.10, 4.6.4, and 5.4.3*).

Moreover, the result in **Figure 5.32** reveals that a mean of 4.27 indicates most respondents who rated this task came in somewhere between very *appropriate* and absolutely *appropriate* positive responses. This further highlight to cloud customers the relevance of negotiating post-migration support when migrating services to/from the cloud environment. However, there is some nuance to the numbers when it comes to the mean (4.27) and median (4.00). The difference between the mean and median shows that even though about 40% of respondents said the "post-migration support" task was very *appropriate*, there were more respondents (45%) who rated it as absolutely a*ppropriate* than (4%) respondents who considered it slightly *appropriate*.

Please rate the importance of each task to be performed in Step 6 (i.e. Service Operation and Validation).

Answered: 113 Skipped: 4

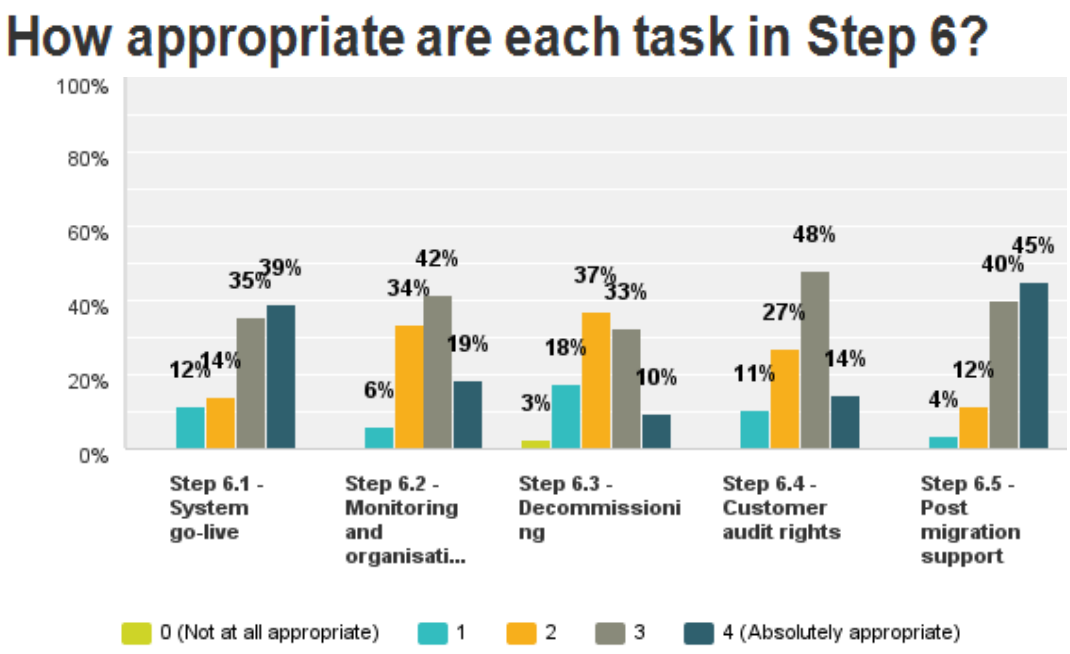


	0 (Not at all important) (1)	1 (2)	2 (3)	3 (4)	4 (Absolutely important) (5)	Total	Weighted Average
Step 6.1 - System go-live	0% 0	12% 13	13% 15	35% 39	41% 46	113	4.04
Step 6.2 - Monitoring and organisational change management	2% 2	4% 5	27% 30	43% 49	24% 27	113	3.83
Step 6.3 - Decommissioning	4% 5	12% 13	35% 39	40% 45	9% 10	112	3.38
Step 6.4 - Customer audit rights	0% 0	16% 18	27% 30	40% 45	17% 19	112	3.58
Step 6.5 - Post migration support	0% 0	5% 6	16% 18	39% 44	40% 45	113	4.13

Basic Statistics

	Minimum	Maximum	Median	Mean	Standard Deviation
Step 6.1 - System go-live	2.00	5.00	4.00	4.04	1.00
Step 6.2 - Monitoring and organisational change management	1.00	5.00	4.00	3.83	0.90
Step 6.3 - Decommissioning	1.00	5.00	3.00	3.38	0.96
Step 6.4 - Customer audit rights	2.00	5.00	4.00	3.58	0.95
Step 6.5 - Post migration support	2.00	5.00	4.00	4.13	0.87

Figure 5.31-Task Evaluation in Step 6 – Importance



	0 (Not at all appropriate) (1)	1 (2)	2 (3)	3 (4)	4 (Absolutely appropriate) (5)	Total	Weighted Average
Step 6.1 - System go-live	0% 0	12% 13	14% 16	35% 40	39% 44	113	4.02
Step 6.2 - Monitoring and organisational change management	0% 0	6% 7	34% 38	42% 47	19% 21	113	3.73
Step 6.3 - Decommissioning	3% 3	18% 20	37% 42	33% 37	10% 11	113	3.29
Step 6.4 - Customer audit rights	0% 0	11% 12	27% 30	48% 54	14% 16	112	3.66
Step 6.5 - Post migration support	0% 0	4% 4	12% 13	40% 45	45% 51	113	4.27

Basic Statistics	Minimum	Maximum	Median	Mean	Standard Deviation
Step 6.1 - System go-live	2.00	5.00	4.00	4.02	1.00
Step 6.2 - Monitoring and organisational change management	2.00	5.00	4.00	3.73	0.83
Step 6.3 - Decommissioning	1.00	5.00	3.00	3.29	0.96
Step 6.4 - Customer audit rights	2.00	5.00	4.00	3.66	0.85
Step 6.5 - Post migration support	2.00	5.00	4.00	4.27	0.80

Figure 5.32-Task Evaluation in Step 6 – Appropriateness

5.11 Evaluation of the Sample Decision Trees

To specifically address ***E03*** and validate the sample decision trees used in the proposed cloud migration decision framework, two questions were developed to examine the comprehensiveness of the model, usefulness and suitability. Regarding the latter, the sample decision trees used in steps (**2.2** and **2.4**) was provided for evaluation by IT practitioners and decision-makers to assess the suitability of the decision-making logic (i.e. relationship between components) used within each task in the context of a typical cloud migration project. The participants were given examples of how to use the decision tree (*see* example in **Figure 5.33**) and were asked to comment during the evaluation session. **Figure**(**s**) **5.34** and **5.35** shows the results of the responses. Across both figures, the measure of dispersion (i.e. standard deviation) in the sample distribution is automatically zero. This is true because there was no dispersion at all in the sample (i.e. Yes response = 100%), hence all the observed values would be the same. The mean would also be the same as this repeated value – no observed value would deviate or differ from the mean.

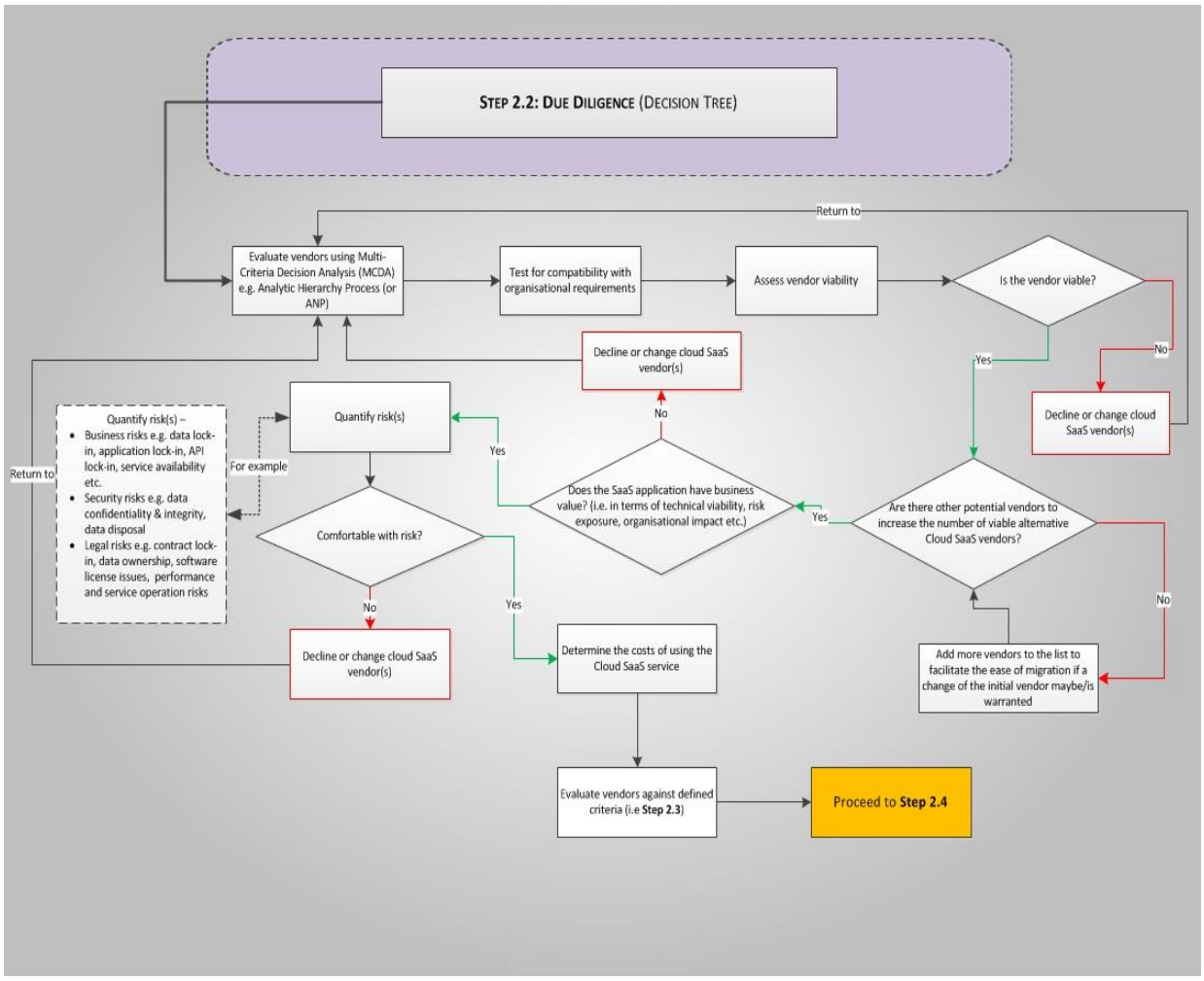


Figure 5.33-Sample Decision Tree for Step 2.2

Answer Choices	Responses	
Yes (1)	**100%**	113
No (2)	**0%**	0
Total		**113**

Basic Statistics				
Minimum 1.00	**Maximum** 1.00	**Median** 1.00	**Mean** 1.00	**Standard Deviation** 0.00

Figure 5.34-Decision Tree Evaluation in Step 2.2

Therefore, overall assessment of the decision trees achieved a high degree of agreement between the participants, as shown in the figures below. The statement that the factors (i.e. details of components) used in the decision-logic is comprehensive and supportive of selecting the cloud computing SaaS service model was strongly supported. All the 113 IT practitioners and decision-makers who expressed a view agreed that the decision tree provides a good reflection of the tasks which are carried out in step 2.2, and as such consider it a useful tool to support the selection of vendor-neutral cloud services and solutions. This finding also suggests that, perhaps, participants who agreed with the above statement may likely find the sample decision trees (*see* **Figure 5.8**) useful as it would reduce the cost in terms of risk assessment, man power (i.e. skills) and time needed to make the correct decision on the selection of interoperable and portable cloud services.

As shown in **Figure 5.35**, IT managers and decision makers strongly (100%) endorsed the statement that the sample decision tree for step 2.4 is an accurate representation of the tasks and relationship between components in decision step – "vendor evaluation and selection". This result confirms that the structure of the proposed novel decision framework makes it simpler and more understandable for decision makers to make informed choices when navigating amongst cloud services and vendors.

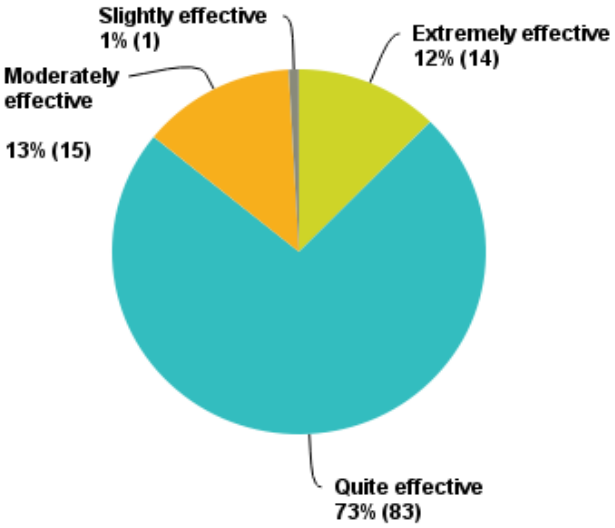
Answer Choices	Responses	
Yes (1)	**100%**	113
No (2)	**0%**	0
Total		**113**

Basic Statistics				
Minimum 1.00	**Maximum** 1.00	**Median** 1.00	**Mean** 1.00	**Standard Deviation** 0.00

Figure 5.35-Decision Tree Evaluation in Step 2.4

5.12 Overall Effectiveness of the Framework

To specifically address ***E04***, participants were asked to rate the effectiveness of the proposed framework. Overall, the framework was assessed for its effectiveness and evaluated for its suitability using 26 ranked closed questions, some of which involved open options for qualitative responses. In general, the model received a high level of support from all stakeholders (i.e. cloud architects, researchers, developers, migration and integration specialists, IT managers, C-level executives etc.). All the participants agreed with the aim of the proposed novel 6-step decision framework in terms of avoiding vendor lock-in risks at the SaaS layer, and to support an informed decision-making process for cloud migration and adoption at the strategic level. The evaluation questionnaire data, so far, shows that survey respondents gave very high ratings overall to almost all the aspects of the proposed 6-step decision framework – i.e. ranging from the sequence and logical order of the decision steps, to the importance of each decision step and tasks with supporting activities, and also the sample decision trees – but only a lesser minority considered the proposed framework to be slightly (1%) *effective* (*see* **Figure 6.30**).



Answer Choices	Responses	
Extremely effective (1)	12%	14
Quite effective (2)	73%	83
Moderately effective (3)	13%	15
Slightly effective (4)	1%	1
Total		**113**

Basic Statistics				
Minimum 1.00	**Maximum** 4.00	**Median** 2.00	**Mean** 2.03	**Standard Deviation** 0.54

Figure 5.36- Overall Effectiveness of the Proposed Framework

From the figure above, a significant majority (73%) of respondents considered the framework to be quite *effective*, while the other 25% combined together rated it as either moderately *effective* (i.e. n = 15) or extremely *effective* (n = 14). Moreover, when looking at the mean (2.03) and median (2) values, it could be observed that some nuance exists. A weighted mean value of 2.03 with a standard deviation of 0.54 signifies that 85% of respondents for this question come from the quite *effective* and extremely *effective* positive responses. Therefore, overall all enterprise IT decision-makers and stakeholders who expressed a view agreed that the proposed decision framework provides a structured methodology to support cloud migration at strategic level to avoid vendor lock-in, and that the lock-in factors addressed at a high level are comprehensive. Stakeholders and IT practitioners who rated the components (i.e. logical order, sequence of steps, importance and propriety of individual tasks and supporting activities) and their relationships as used within the evaluation makes it fair for author to denote herein that; "the novelty of the proposed framework lies in its ability to make it simpler and more understandable for decision makers to avoid vendor lock-in challenges in cloud migration." For instance, in terms of the suitability of activities and tasks performed to avoid vendor lock-in risks, the evaluation result from practitioners confirmed respondents strongly agreed that using the framework could reduce the vendor lock-in challenges and risks affecting enterprise cloud adoption and migration decisions. To further substantiate the aforesaid, the participants were asked if the sample decision trees provide useful tools to support cloud migration decision making (as in vendor evaluation and service selection step 2); all agreed.

While **Figure 5.36** shows that all the participants agree that the framework is *effective*, author also included an open-ended question in questionnaire, to collect qualitative data from IT practitioners and decision-makers in the form of suggestions, comments and feedbacks which would help improve the frameworks. The results obtained in this regard are represented in the screen dump shown in **Figure 5.37**, to substantiate the aforesaid. 15 qualitative responses were received from participants who contributed in the evaluation survey. However, 3 responses were removed (due to incomplete/invalid responses and inconsistent comments with errors etc.) to maintain consistency with equal validity in the data analysis. An example of qualitative responses received as per the overall effectiveness and practicability of the proposed framework is depicted below.

#	Responses
1	I presume this framework will support the identification of cloud lock-in pitfalls during migration as it provides an in-depth analysis of the decisions (or steps) required to avoid it in a systematic way.
2	By taking 6 decision steps and their corresponding activities within the proposed cloud migration framework, organisations will be better poised to migrate their IT systems and applications into, around and out of the cloud as designed with less fear of proprietary lock-in.
3	In my opinion, the derivation of the decision steps and tasks within the framework are generalised to favour enterprise-wide interoperability and portability requirements for SaaS implementation in an organisation. It is suggested to identify necessary tools to meet those needs and establish criteria for evaluating what is appropriate for the type of corporate data involved.
4	In terms of usability and practicability, I can foresee the proposed decision framework being used to assist with creating effective cloud migration strategies; defining interoperability and portability requirements, delivery architecture, creating the migration plans, designing the contractual and SLA plans, and more. Good effort I must say; overall the survey was very absorbing and impressive indeed. Thank you for sharing your research
5	Overall, the decision framework captures the core migration requirements for cloud computing, and can act as intermediary to support teams and client during cloud-to-cloud/on-premise migration projects
6	The proposed framework has been developed using a pragmatic cloud strategy and with a proven cloud road-map to maximize the benefits of cloud with minimal risk exposure to vender lock-in. It is evident, that the authors' indeed have a passion for cloud with a good understanding of the vender lock-in problem domain as well as sound knowledge of different cloud architecture environments.
7	This is well thought-out and presented model of a decision framework to support cloud migration with minimal risks of vendor lock-in. I can already see it being useful to SMEs considering cloud migration but are unaware of the effect of the lock-in problem. I suppose a publication accompanies this proposal, because it would be interesting to see the dynamics and scope within each phase is supported by relevant literature. Overall, well done!
8	Impressive approach to tackling the vendor lock-in problem. It might be interesting to use the already developed processes to build a support system to aid organisations cloud adoption strategy
9	Overall, it is quite an impressive piece of work. Good luck
14	Overall, this is a well thought out research work with huge consultative benefits for organisations.
15	As a comment, since the proposed framework is aimed at minimising lock-in risks at SaaS layer of the cloud stack it is equally important that special attention be payed to data lock-in and integration issues.

Figure 5.37-Qualitative survey responses from IT Practitioners

For example, participants in favour of the proposed decision framework are seen in comments *#2*, ***#4***, *#5* and ***#7***. On the other hand, while it is reassuring to receive such high-level comments one striking comment from an IT practitioner seals this PhD study in terms of its novel contribution to knowledge;

"*The proposed framework has been developed using a pragmatic cloud strategy and with a proven cloud roadmap to maximise benefits of cloud and minimise vendor lock-in risk exposure. It is evident that the author indeed has a passion for cloud computing with a good understanding of the lock-in problem domain, as well as sound knowledge of different cloud architecture environments*" – *see* comment ***#6***.

In fact, the main purpose of this evaluation study was set out to explore the views of IT practitioners and key enterprise decision-makers on the one hand, and on the other, to establish the extent to which the proposed decision framework and its attributes is considered effective in terms of its practicability to avoid the vendor lock-in risks in cloud migration. The figures and statistical chart tables presented in this chapter so far, including the qualitative comments and feedbacks received, represent a healthy belief and strong acceptance/conviction in the frameworks sequence, suitability, *importance* and *propriety* in addressing the vendor lock-in problem. No suggestions were made for the future development of the novel 6-step decision framework for cloud migration, apart from the comment highlighted in red ink (i.e. #3, #8, and #15) as shown in **Figure 5.37**. Nonetheless, the comments labelled #1, #9 and #14 have been categorised as feedbacks or remarks made by survey participants.

5.13 Chapter Summary

The validation of the proposed six-step decision framework to avoid vendor lock-in risks in cloud migration was achieved by conducting a survey. The aim of the validation was to examine the appropriateness (i.e. clarity), importance (i.e. usability and suitability) and effectiveness (i.e. practicality) of using the proposed novel 6-step decision framework and the supporting strategies (discussed in *Section 4.6*). The survey questions presented herein have been grouped by decision steps, supporting tasks and decision trees to address the main evaluation objectives and the questions that were raised in the preceding section of this chapter. Findings for each evaluated migration steps (1–6) and corresponding task in terms of their appropriateness, importance and suitability were presented in context of the respective steps within the framework as comprehensively shown in the succeeding *sub-sections (6.11 – 6.15)*. Since that drawing conclusions based on results that are inaccurate (i.e., not statistically significant) is risky. The evaluation results demonstrates that the proposed framework to mitigate vendor lock-in risks will effectively help cloud service consumer to make informed decisions during the replacement or migration of IT systems to the cloud. For example, to statistically address ***EO.1*** each decision step is questioned in terms of its appropriateness for application migration to the cloud. The results from *Section 5.13–5.14* meets the first evaluation objective since it provides a good synopsis of the overall framework sequence and logic in the decision to mitigate vendor lock-in risks when migrating to cloud-based SaaS services. Whereas to address ***EO.2*** and ***EO.3***, findings for each decision step and supporting activity in terms of their importance, suitability, and their relationships (i.e. decision tree) is presented in context of the respective decision point as shown in the *Section 5.14–5.16* respectively.

To sum up, in terms of *appropriateness*, the sequence and logical order of steps within the framework are evaluated for general understand-ability by formulating questions regarding each step, activity, and their relationships (refer to step 2.2 and 2.4 as an example). The questionnaire results from *Section 5.14* and *Section 5.15* respectively, confirms the propriety of the proposed framework. As can be drawn from figures, the appropriateness and logical order of steps within the framework is perceived by respondents as very appropriate, while the *importance* of each step and supporting task within the framework is ranked by most respondents as absolutely important. This finding is unsurprising but expected as the order of steps and names of supporting tasks within the proposed framework is based on many available vendor-specific and vendor-independent methodologies – including frameworks and guidelines for replacing enterprise systems with cloud-based services, migrating legacy systems to the cloud, or migrating applications in the cloud (i.e. inter-cloud migration). Hence, this further ensures that our proposal allows for better understanding of the decisions involved in avoiding vendor lock-in risks. With respect to the *suitability* of each decision step (1–6) and their corresponding relationships between tasks and outcomes, the results from **Figure(s) 5.32–5.35** reveals that the clear majority of survey respondents found the sample decision

tree to be either a good reflection (100%) or an accurate representation (100%) of the tasks performed in step 2. This finding is consistent with a higher-level analysis in our previous study (Opara-Martins et al. 2016) and thus supports the suggestion that the proposed framework is a valuable research contribution in terms of clearly guiding enterprise cloud SaaS adoption strategy with reduced risks of vendor lock-in. Moreover, the questionnaire evaluation result in **Figure 5.36** confirms and substantiates the aforesaid by painting a similar picture regarding the overall ***effectiveness*** of our proposal. According to **Figure 5.36**, the clear majority of study participants who evaluated the framework think it will support and guide organisations' in making informed cloud migration decisions to avoid vendor lock-in. Further, qualitative survey and suggestions provided by participants have also been taken into consideration for further refinement and improvement. So far, consensus opinion from the survey respondents has shown relevance of all decision steps, supporting tasks, and outcome(s) the proposed framework comprises. The validation technique based on the statistical analysis and findings have also showed and confirmed that the proposed decision framework and supported strategies are holistic and provide support for informed cloud computing migration initiatives and adoption to avoid vendor lock-in risks. To further substantiate, the results from the empirical data analysis in *Section 4.5* also sheds some light in this aspect by establishing that the lock-in risk factors and sub-factors identified through the primary *(in Section 2)* and secondary systematic literature research *(in Section 3)* are important in terms of cloud migration and adoption decision making.

Therefore, while the discussions in this section have been limited to the four main evaluation objectives identified in *Section 6.1*, the aspect of the relationships between decisions steps have not been sufficiently discussed herein. Nonetheless, several relationships exist within the framework. Paramount amongst them is the relationship between the six main decision steps and their complementary activities. The understand-ability of this relationship within the framework has been reflected in the results from **Figure(s) 5.32–5.34** respectively. Remember, in **Figure 5.34** and **Figure 5.35** author used a decision tree sample from step 2 to show this connection, and in **Section 5** this relationship is concisely discussed using decision Step 1 and Step 2 as examples. In other words, what this means essentially is that selecting any step within the framework has a direct or indirect impact to the possible outcomes in other decisions (step) and tasks. Overall, the results of this evaluative study can be understood within the context of authors existing work (Opara-Martins et al, 2016; Opara-Martins et al. 2015a; Opara-Martins et al. 2015b; Opara-Martins et al. 2014) as re-enforcing authors arguments that decision makers should consider the multi-dimensional aspects of vendor lock-in and its impact on existing systems and data when making informed decisions pertaining to the adoption and migration of cloud SaaS services.

Chapter Six

6. Conclusion

Cloud computing adoption and migration is a topical issue, and there is significant interest from academia and industry in using cloud-based services and solutions. As academics, we are uniquely positioned to offer unbiased advice and expertise to enterprises that are interested in consuming or using new technologies such as cloud computing. Therefore, the work presented herein is rooted in academic research and fills a gap in the current cloud computing literature. It also provides a vendor-neutral expertise and proposal framework for companies that are interested in deploying or migrating to cloud-based SaaS environments. This PhD research study is concerned with supporting the decision-making process to avoid vendor lock-in risks for cloud-to-cloud migration and/or migrating/replacing on-premise IT systems with cloud-based (SaaS) alternatives.

In this thesis, a comprehensive analysis of vendor lock-in problems was discussed and the impact to companies because of migration to cloud computing was explored. Vendor lock-in affects the application and data migration in cloud computing. Therefore, by improving the interoperability, portability, integration and standards of cloud applications (i.e., the degree of effectiveness and efficiency of a migration) organisations can reduce the risks of vendor lock-in. Migration to the cloud environment is not without pitfalls, and is fraught with vendor lock-in challenges which may affect the overall migration process. A survey was conducted and revealed that the cloud paradigm has greatly impacted on many organisations after migrating IT and business applications to the cloud due to the vendor lock-in problem. The result in **Figure 4.3** shows that many companies have adopted cloud services without being aware of the vendor lock-in problem. In fact, the study has shown also that, while organisations are eager to adopt cloud computing due to its benefits, there is equally an urgent need for avoiding vendor lock-in risks. Moreover, the results of our study have highlighted customers' lack of awareness of proprietary standards which prohibit interoperability and portability when procuring services from vendors. The complexity and cost of switching providers is often under-appreciated until implementation. Business decision makers are often unaware of how to tackle this issue. Our findings offer cloud computing consumers, service providers, and industry practitioners a better understanding of the risk of lock-in embedded in the complex, technologically interdependent and heterogeneous cloud systems. In this respect, our research points to the need for more sophisticated policy approaches that take a system-wide perspective to alleviate the current vendor lock-in problem which affects interoperability and portability.

Further, our findings show that within many organisations in the study, a lack of clarity on the problem space of vendor lock-in still pervades. This lack of knowledge poses a significant barrier to obscure the potential effect the vendor lock-in problem could have on enterprise applications migrated

to and operating in cloud platforms. To date, the expertise and technological solutions to simplify such transition and facilitate good decision making are limited. Hence, to be protected against such risks when migrating to the cloud environment, companies require standards, portability, and interoperability to be supported by providers. However, this is currently difficult to achieve as explored in this thesis. Fundamentally, the difficulty is attributed to the vendors' APIs which control how cloud services are harnessed, as cloud APIs are not yet standardized, making it complex for customers to change providers. Some cloud providers are concerned with the loss of customers that may come with standardisation initiatives which may then flatten their profits and do not regard the solution favourable. Therefore, we propose the following strategic approaches to address the issues: (i) create awareness of the complexities and dependencies that exist among cloud-based solutions; (ii) assess providers' technology implementation such as API and contract for potential areas of lock-in; (iii) select vendors, platforms, or services that support more standardised formats and protocols based on standard data structures; and (iv) ensure there is sufficient portability. Furthermore, this thesis also explores interoperability and portability constraints which affect enterprise application migration and adoption of SaaS clouds. Being that data is the cornerstone of successful cloud application deployment, to this end, we proposed a decision framework to support cloud SaaS migration in enterprises. The framework through its step-by-step approach provides guidance on how to avoid being locked to individual cloud service providers. This reduces the risk of dependency on a cloud vendor for service provision, especially if data portability, as the most fundamental aspect, is not enabled. Thus, the corresponding framework can be used to aid cloud service consumers in terms of better understanding the vendor lock-in risks specific to core components (or constituents) of cloud SaaS services. Also, the framework will also educate the users, giving them an awareness of the problem space of cloud vendor lock-in. Besides, decision frameworks and models to support informed decisions as per cloud computing adoption and migration in the enterprise is an interesting research area that requires the support of results from surveys and quantitative analysis. Likewise, in this thesis, author identifies the six key decision steps for cloud SaaS migration and IT success, and explains how these six steps with their supporting activities and strategies can be followed and implemented to avoid vendor lock-in challenges for a successful IT project delivery and cloud migration experience. The cost of not having this framework will put organisations and businesses at the proprietary lock-in risk including socio-economic risks. To take advantage of cloud computing environments and protect existing investments to legacy systems, enterprises are eager to replace and/or migrate legacy systems to the cloud. So far, the amount of research effort in this aspect of cloud computing have focused more on decision making support systems for cloud migration in enterprise as benefits, risks, costs, and organisational and socio-technical factors must be considered before migration. Decisions to migrate enterprise business systems to the cloud environment (i.e. cloud migration) can be complicated as evaluating the benefits, risks and costs of using cloud computing is far from straightforward. Organisational and socio-technical factors must also be

considered during the decision-making process as the transition to the cloud is likely to result in noticeable changes to how systems are developed and supported. However, the focus of the thesis is on the socio-technical, business, and legal challenges related to cloud SaaS lock-in.

To test and validate the frameworks attributes in tackling the lock-in problem, author sent our evaluation surveys to IT practitioners, collected feedback and analysed statistical data to confirm that the decision steps and corresponding activities within the proposed framework can meet organizational goals, user satisfaction and stakeholders' requirements. Furthermore, the positive response received from the evaluation result of the framework from our main target audience, in the context of their day-to-day job, help to build confidence on the effectiveness of the proposed novel 6-step decision framework and its lifecycle process for managing vendor lock-in risks in cloud migration. Additionally, the framework evaluation results show it aims to support informed decision making for adopting SaaS within already existing IT environment and/or migrating to cloud-based SaaS solutions that aligns with the business and IT strategy of an organisation where vendor lock-in risk is the main challenge and, flexibility (i.e. switching ease) and vendor-neutrality (i.e. standards-based) are valuable objectives. In other words, the proposed 6-step decision framework is seen as a practical contribution towards advancing the state-of-the-art on the analysis, selection, and use of cloud-based technologies within existing enterprise environment. In turn, this will support the advancement of SaaS migration and cloud computing adoption, in general.

6.1 Contributions Revisiting

The aim of this thesis was to develop a novel framework to avoid vendor lock-in risks in cloud (SaaS) migration. This was to be achieved by

1. Exploring views of professional IT practitioners on issues associated with cloud vendor lock-in.
2. Identifying, analysing and exploring the technical, legal, and business issues associated with cloud vendor lock-in.
3. Identifying policy and industry recommendations that could potentially steer the development of a vendor-neutral cloud marketplace.

    a. Identify standards that support interoperability between different cloud providers network.

    b. Identify standards that facilitate the portability of data from one vendor to another.

    c. Examine limitations in existing cloud service contracts and Service Level Agreement (SLA) that fail to tackle the risks of vendor lock-in, and review their implications for businesses adopting cloud computing

4. Systematic reviewing of relevant literature on typical cloud providers' standard contract terms of services and SLAs as an attempt to identify the contractual issues which need to be addressed in order to enable the cloud-to-cloud migration or on-premise-to-cloud-based SaaS application modernisation.
5. Developing a novel decision framework to avoid vendor lock-in risks in cloud (SaaS category) migration.
6. Evaluating the proposed framework based on expert opinions, enterprise decision-makers and IT practitioners' review

The first four (i.e. 1 – 4) were met and extensively discussed in Chapter 2, Chapter 3 and Chapter 4. Objectives 5 and 6 were achieved in Chapter 5 and Chapter 6, respectively. However, one of the limitations of the proposed decision framework as per objective 6 is the lack of systematic assistance and automated tool to support the decision-making process to avoid the lock-in problem within existing enterprise environment. Collectively, Chapter 3, Chapter 4, Chapter 5 and Chapter 6 are the heart of this PhD thesis. It comprehensively details both strategic and tactical activities as well as initiatives for enterprise decision makers implementing hybrid cloud SaaS solutions. It covers all the essential technical, business-related and legal considerations for avoiding vendor lock-in challenges in cloud deployment including integration, compatibility, standards, APIs, interoperability, portability, connectivity, security, governance, compliance and privacy. It provides specific guidance and best practices for enterprise decision-makers and cloud customers in each of these areas, but with a particular focus on vendor lock-in.

6.2 Suggestions for Future Research Directions

This thesis had demonstrated that vendor lock-in challenges cannot be completely (especially within the nascent but constantly evolving cloud computing environment) eradicated in its entirety, but its associated risks can be mitigated to a reasonable risk acceptance level. A considerable amount of further work must be done if this is to be achieved; however, the following suggestions are therefore provided.

A holistic systematic risk assessment tool for application and data migration in the cloud SaaS environment, which incorporates the various lock-in challenges discussed in this thesis and guides enterprise decision-makers and stakeholders through informed decision-making during the migration (or replacement of on-premise IT systems to the cloud) process, is a natural continuation of this work. This tool should provide a systematic means (or assistance) to support the decision-making process through Step 1 – Step 6 of the proposed novel framework, to assist cloud service consumers to select cloud (SaaS) services and cloud a service provider that fits their risk profile best. Moreover, such tool for assessing lock-in risks should be based on existing frameworks such as ENISA, ITIL, COBIT,

ISO, TOGAF etc. and complement them to provide enterprises and cloud customers with a practical tool to support informed decision-making for cloud migration. The implementation of such tool should embody a risk assessment approach such that the evaluation and selection (refer to *Section 6.1 – 6.3*) of cloud service providers/services is carried out for a specific migration case. In this respect however, further research on how to technically avoid lock-in when moving between different vendor platforms and cloud deployment models (since by switching the provider the initial ex-ante investments could be largely lost and new investments required to adapt the software and retrain employees will also be necessary, thus exceeding the benefits of the provider change), and a deeper investigation in the interoperability and portability of cloud providers is also necessary.

Furthermore, given the complex business challenges and risks of vendor lock-in involved in cloud computing initiatives, still there are concerns such as meeting technical and legal requirements (refer to *Section 3.3.2*), security (refer to *Section 4.5.3*), ease of integration – due to heterogeneity roots in cloud environments (refer to *Section 2.9.2*), functionality and compatibility among SaaS consumers in adopting and migrating to cloud environments. To further address these problems, future work because of this PhD study recommends: firstly, that each enterprise has to assess its application portfolio based on its business imperatives, technology strategy, legal compliance, and lock-in risk appetite before embarking on a migration into the clouds using different deployment models (private, public, community, and hybrid clouds). With such assessment that involves multiple competing criteria of varied nature, impact and priority; secondly, it will be interesting to demonstrate in future works how a multi-dimensional statistical approach using the Analytic Hierarchy Process (AHP), for example, as already illustrated and suggested in ***Step 2*** (refer to **Figure 5.2**), can be used to help decide and aid informed decision-making on which, if any, of an enterprise application(s) belong in the cloud SaaS environment. Such automated analysis and/or solution may exploit state-of-the-art; interoperable and portable standards, configurable management standards and frameworks, security standards and frameworks, security software and secure model management technology. Moreover, it should cover different switching/changing cloud vendor scenarios (*refer to Section 3.4.1 – 3.4.3*), integrating different cloud services and on-premise systems (i.e. hybrid scenarios), and various access control scenarios involving external, web-based and programmatic user authentication protocols and APIs.

References

Abu-Libdeh, H. Princehouse, L. and Weatherspoon, H., 2010. RACS: a case for cloud storage diversity, in 1st ACM SoCC '10, 2010, pp. 229–240.

Ahronovitz, M. et al., 2010. Cloud Computing Use Cases: Introducing Service Level Agreements, *Use Cases Discussion Group*, White Paper V4.0 [online] http://www.cloud-council.org/Cloud_Computing_Use_Cases_Whitepaper-4_0.pdf [Accessed 8 February 2015].

Aleem, A. and Sprott, C.R., 2013. Let me in the Cloud: Analysis of the Benefit and Risk Assessment of Cloud Platform, Journal of Financial Crime, Vol. 20 Issue: 1, pp.6-24. http://dx.doi.org/10.1108/13590791311287337

Alhamad, M., Dillon, T. and Chang, E., 2010. Conceptual SLA framework for cloud computing. In *Digital Ecosystems and Technologies (DEST), 2010 4th IEEE International Conference on* (pp. 606-610) April. IEEE.

Alkhalil, A., Sahandi, R. and John, D., 2013. Migration to Cloud Computing-The Impact on IT Management and Security, in *1st International Workshop on Cloud Computing and Information Security*, Atlantis Press.

Alkhalil A, Sahandi R, John D., 2014. Migration to Cloud Computing: A Decision Process Model. In *Central European Conference on Information and Intelligent Systems* (p. 154) January. Faculty of Organization and Informatics Varazdin.

Amazon Opsworks, 2016. Available from: https://aws.amazon.com/opsworks/ [Accessed 1 August 2016].

Andrikopoulos, V., Binz, T., Leymann, F. and Strauch, S., 2013. How to Adapt Applications for the Cloud Environment: Challenges and Solutions in Migrating Applications to the Cloud, *Springer Computing Journal*, vol. 95, no. 6, pp. 493-535.

Ardagna, D., Di Nitto, E., Casale, G., Petcu, D., Mohagheghi, P., Mosser, S., Matthews, P., Gericke, A., Ballagny, C., D'Andria, F. and Nechifor, C.S., 2012. Modaclouds: A model-driven approach for the design and execution of applications on multiple clouds. In Proceedings of the 4th International Workshop on Modelling in Software Engineering (pp. 50–56). IEEE Press.

Armbrust, M., Fox, A., Griffith, R., Joseph, A.D., Katz, R., Konwinski, A., Lee, G., Patterson, D., Rabkin, A., Stoica, I. and Zaharia, M., 2009. Above the Clouds: A Berkeley View of Cloud Computing, *Communications of the ACM*, vol. 53, no. 4, pp. 50- 58.

Aureli, L., Pierfranceschi, A. and Wache, H., 2012, June. Enterprise architectures for cloud computing. In *Cloud Computing (CLOUD), 2012 IEEE 5th International Conference on* (pp. 979-980). IEEE.

Aversa, R., Tasquier, L., and Venticinque, S., 2012. Management of Cloud Infrastructures through Agents. In: 2012 3rd International Conference on Emerging Intelligent Data and Web Technologies (EIDWT), pp. 46-53 IEEE.

Babar, M.A. and Chauhan, M.A., 2011. A tale of migration to cloud computing for sharing experiences and observations. In *Proceedings of the 2nd international workshop on software engineering for cloud computing* (pp. 50-56) May. ACM.

Badger, Lee, Grance, Tim, Patt-Corner, Robert, & Voas, Jeff., 2011. Cloud Computing Synopsis and Recommendations, [draft] (Special Publication 800-146). National Institute of Standards and Technology [online] Available from: http://csrc.nist.gov/publications/drafts/800-146/Draft-NIST-SP800-146.pdf [Accessed 24 January 2015].

Banerjee, J., 2012a. Moving to the Cloud: Workload Migration Techniques and Approaches. In: *High Performance Computing (HiPC), 2012 19th International Conference on*, vol., no., pp.1,6, 18-22 Dec. 2012. doi: 10.1109/HiPC.2012.6507519

Banerjee, J. Debasis, Choudhuri, R. and Swift, L.K., 2012b. Accelerate to Green IT - A Practical Guide to Application Migration and Re-hosting, developerWorks, July 2012. Available from: https://www.ibm.com/developerworks/linux/library/l-greenit/l-greenit-pdf.pdf [Accessed 24 May 2015].

Bang, S.K., Chung, S., Choh, Y. and Dupuis, M., 2013, October. A grounded theory analysis of modern web applications: knowledge, skills, and abilities for DevOps. In *Proceedings of the 2nd annual conference on Research in information technology* (pp. 61-62). ACM.

Baryannis, G., Garefalakis, P., Kritikos, K., Magoutis, K., Papaioannou, A., Plexousakis, D. and Zeginis, C., 2013, April. Lifecycle management of service-based applications on multi-clouds: a research roadmap. In *Proceedings of the 2013 international workshop on Multi-cloud applications and federated clouds* (pp. 13-20). ACM.

Beserra, P.V., Camara, A., Ximenes, R., Albuquerque, A.B., Mendonca, N.C., 2012. Cloudstep: A step-by-step decision process to support legacy application migration to the cloud. In: Maintenance and Evolution of Service-Oriented and Cloud-Based Systems (MESOCA 2012) Workshop. pp. 7–16. IEEE.

BCS, 2012. Cloud Computing: Moving IT out of the office. [online] Available from: http://www.bcs.org/upload/pdf/cloud-computing.pdf [Accessed 19 February 2015].

Beggs A, Klemperer P., 1992. Multi-period competition with switching costs. *Econometrical: Journal of the Econometric Society*, pp.651-666.

Benatallah, B., Motahari-Nezhad, H.R., Ferro, A., Boerger, E., 2008. Service oriented architecture: Overview and Directions. In: Advances in Software Engineering, vol. 5316/2008, pp.116 -130.

Bernstein, P., 1996. Middleware: A model for distributed systems services. In: Commun. ACM, pp.86 -98

Bershad, B.N., Ching, D.T., Lazowska, E.D., Sanislo, J. and Schwartz, M., 1987. A remote procedure call facility for interconnecting heterogeneous computer systems. *IEEE Transactions on Software Engineering*, (8), pp.880-894.

Binz T, Breiter G, Leyman F, Spatzier, T., 2012. Portable cloud services using tosca. IEEE Internet Comput 3:80–85

Binz, T. Leymann, F. and Schumm D., 2012. CMotion: A Framework for Migration of Applications into and between Clouds, Proc. Int'l Conf. Service-Oriented Computing and Applications, IEEE Press, pp. 1–4.

Binz, T., Breitenbücher, U., Kopp, O. and Leymann, F., 2014. TOSCA: portable automated deployment and management of cloud applications. In *Advanced Web Services* (pp. 527-549). Springer New York.

Blair, G., Paolucci, M., Grace, P. and Georgantas, N., 2011. Interoperability in complex distributed systems. *Formal Methods for Eternal Networked Software Systems*, pp.1-26.

Boughzala, B., Ben Ali, R., Lemay, M., Lemieux, Y., Cherkaoui, O., OpenFlow Supporting Inter-Domain Virtual Machine Migration, Proceedings. In 2011 Eighth International Conference on Wireless and Optical Communications Networks (WOCN), pp.1–7, 24– 26 May 2011.

Bozman, J., 2010. Cloud Computing: The Need for Portability and Interoperability [online]. Available from: http://delimiter.com.au/wp-content/uploads/2010/10/The-need-forportability-and-interoperability-IDC.pdf [Accessed on 6 March 2014].

Bradshaw, D., Folco, G., Cattaneo, G. and Kolding, M., 2012. Quantitative estimates of the demand for cloud computing in Europe and the likely barriers to up-take, IDC Interim Tech. Report. SMART 2011/0045 [online] Available from: http://cordis.europa.eu/fp7/ict/ssai/docs/study45-d2-interim-report.pdf [Accessed 29 December 2014].

Bradshaw, S. Millard, C. Walden, I., 2010. Contracts for Clouds: Comparison and Analysis of the Terms and Conditions of Cloud Computing Services, Queen Mary School of Law Legal Studies Research Paper 63.

Brambilla, M., Cabot, J. and Wimmer, M., 2012. Model-Driven Software Engineering in Practice. Morgan & Claypool Publishers, p. 182.

Breitenbucher, U., Binz, T., Kèpes, K., Kopp, O., Leymann, F., and Wettinger, J., 2014. Combining Declarative and Imperative Cloud Application Provisioning based on TOSCA. In IC2E. IEEE.

Bryman, A., 2012. Social research methods. 4th Ed. [Online]. Oxford: Oxford university press. Available from: http://books.google.com/books?hl=en&lr=&id=vCq5m2hPkOMC&oi=fnd&pg=PP2&dq=Social+research+methods&ots=CJUdImaXrw&sig=DLECqyvMqK0DQpbuHTxuUAOXZPA. Accessed: 27 September 2015.

Burns, M., 2012. Cloud-based ERP: the risk of Vendor Lock-in. In *Emerging Issues and Technologies for ERP Systems*

Business Process Model and Notation (BPMN) Version 2.0. OMG (2011)

Buyya, R., Yeo, C. S., Venugopal, S., Broberg, J. and Brandic, I. 2009. Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility, *Future Generation computer systems*, vol. 25, no. 6, pp. 599-616.

Buyya, R., Ranjan, R., Calheiros, R.N., 2010. InterCloud: Utility-oriented federation of cloud computing environments for scaling of application services, *Proceedings of the 10th International Conference on Algorithms and Architectures for Parallel Processing* (ICA3PP 2010), Busan, South Korea. Springer: Germany, 21–23 May; 328–336.

Buyya, R., Vecchiola, C., and Selvi, S. T. (2013). Mastering Cloud Computing: Foundations and Applications Programming. Morgan Kaufmann Publishers Inc., San Francisco, CA, USA, 1st edition.

Cabral, L. (2012), Switching costs and equilibrium prices, New York University: [online] Available from: https://archive.nyu.edu/jspui/bitstream/2451/31545/2/Cabral-SwitchingCostsandEquilibriumPrices_Mar2012.pdf. [Accessed 11 April 2014].

Carraro, G. 2008b. Monetization: the next frontier of SaaS/S+S architecture. Microsoft Corporation, blogs.msdn.com/gianpaolo/archive

Casemore, B., 2014. The Rise of the Hybrid WAN: Meeting the Challenge of the Cloud [Online]. Available from: https://www.silver-peak.com/sites/default/files/infoctr/idc_wp_rise-of-the-hybrid-wan.pdf [Accessed 8 November 2016].

Catteddu D. and Hogben, G. "Cloud computing - benefits, risks and recommendations for information security," European Network and Information Security Agency, Tech. Rep., 2009.

CFEngine, 2016. Available from: https://cfengine.com/product/what-is-cfengine/ [Accessed 1 August 2016].

Chalamalasetti, S.R., Lim, K., Wright, M., AuYoung, A., Ranganathan, P. and Margala, M., 2013, February. An FPGA memcached appliance. In *Proceedings of the ACM/SIGDA international symposium on Field programmable gate arrays* (pp. 245-254). ACM.

Chauhan, M.A. and Babar, M.A., 2011, July. Migrating service-oriented system to cloud computing: An experience report. In *Cloud Computing (CLOUD), 2011 IEEE International Conference on* (pp. 404-411). IEEE.

Chauhan, M.A., and Babar, M.A., 2012. Towards process support for migrating applications to cloud computing. In: 2012 International Conference on Cloud and Service Computing. pp. 80–87. IEEE Computer Society.

Chen, D., Doumeingtsb, G., Vernadatc, F., 2008. Architectures for Enterprise Integration and Interoperability: Past, present and future. In: Comput. Ind., vol. 59, no. 7, pp.647 -659

Chetan, S., Kumar, G., Dinesh, K., Mathew, K. and Abhimanyu, M.A., 2010. Cloud computing for mobile world. *available at chetan. ueuo. com*.

Chien, C. S., and Chien, J., 2011. Insight to Cloud Computing and Growing Impacts, Information Computing and Applications. Springer, Vol 105, pp 250-257.

Chong, F., and Carraro, G., 2006. Architecture Strategies for Catching the Long Tail. Microsoft Corporation.

Chow, R., Golle, P. Jakobsson, M. Shi, E. Staddon, J. Masuoka, R. and Molina, J., 2009. Controlling data in the cloud: outsourcing computation without outsourcing control. In: Proceedings of the 2009 ACM workshop on Cloud computing security, ser. CCSW '09. New York, NY, USA: ACM, 2009, pp. 85–90. [online]. Available: http://doi.acm.org/10.1145/1655008.1655020

Cisco Systems, 2010. Planning the Migration of Enterprise Applications to the Cloud, A Guide to your migration Options and Best Practices, *Technical report* [online] http://www.cisco.com/en/US/services/ps2961/ps10364/ps10370/ps11104/Migration_of_Enterprise_Apps_to_Cloud_White_Paper.pdf [Accessed 1 December 2014].

Citrix, 2016, Citrix Systems, Inc. Xen hypervisor. [online] Available from: http://www.xen.org [Accessed 7 January 2016].

Citrix, 2012. Cloud Platform Deployment Reference Architecture. Citrix CloudPlatform Version 3.0.x [online] Available from: https://www.citrix.com/content/dam/citrix/en_us/documents/oth/cloudplatform-deployment-reference-architecture.pdf [Accessed on 8 May 2015].

Clark, K., 2015. Integration Architecture: Comparing Web APIs with Service-Oriented Architecture and Enterprise Application Integration'. *IBM DeveloperWorks*, Technical Report. [online] Available from: http://www.ibm.com/developerworks/websphere/library/techarticles/1503_clark/1305_clark-pdf.pdf [Accessed 2 May 2015].

Clement, S.J., McKee, D.W. and Xu, J., 2017, April. Service-Oriented Reference Architecture for Smart Cities. In *Service-Oriented System Engineering (SOSE), 2017 IEEE Symposium on* (pp. 81-85). IEEE.

Cloud Data Management Interface (CDMI) Storage Networking Industry Association (SNIA).

Cloud Industry Forum, 2014. The Normalisation of Cloud in a Hybrid IT market – UK Cloud Adoption Snapshot & Trends for 2015, *Cloud UK, Paper 14* [online] http://www.aspect.com/globalassets/images/uk-documents/aspect---cif-wp.pdf [Accessed 17 November 2014].

Cloud Industry Forum (CIF), 2015. Making sense of Hybrid IT: Cloud computing now the norm in a predominantly Hybrid IT Market [online]. Available from: http://cloudindustryforum.org/news/582-cloudcomputing-now-the-norm-in-a-predominantly-hybrid-it-market [Accessed 11 February 2016]

Conway, G., Curry, E., 2013. The IVI Cloud Computing Life Cycle. In: Ivanov, I.I., van Sinderen, M., Leymann, F., Shan, T. (eds.) CLOSER 2012. CCIS, vol. 367, pp. 183–199. Springer, Heidelberg.

Cordys.com, 2015. Cordys Process Factory [online]. Available from: http://www.cordysprocessfactory.com [Accessed 1 June 201].

Cowan, R. 1991. Tortoises and hares: Choice among technologies of unknown merit. *The Economic Journal, Jan. 1991*. [online]. Available from: http://links.jstor.org/sici?sici=0013-0133(199107)101%253A407%253C801%253ATAHCAT%253E2.0.CO%253B2-S [Accessed 16 September 2014].

Coyne, L., Hajas, T., Hallback, M., Lindstrom, M. and Vollmar, C., 2016. IBM Private, Public, and Hybrid Cloud Storage Solutions [Online]. Available from: http://www.redbooks.ibm.com/redpapers/pdfs/redp4873.pdf [Accessed 18th June 2016]

Crago, S. P., and Walters, J.P., 2015. Heterogeneous Cloud Computing: The Way Forward. In IEEE Computer Society (Cloud Cover). Available from: http://s3.amazonaws.com/ieeecs.cdn.cci/documents/07030253.pdf [Accessed 7th March 2016].

Creeger, M., 2009. CTO roundtable. Communications of the ACM, 52, 50.

CSA, 2009. Security Guidance for Critical Areas of Focus in Cloud Computing, Technical report, Cloud Security Alliance.

Cusumano, M., 2010. Cloud computing and SaaS as new computing platforms. Communications of the ACM, 53, 27–29.

Delaet, T., Joosen, W., Van Brabant, B., 2010. A survey of system configuration tools. In: Drunen, R. van (ed.) 24th Large Installation System Administration conference (LISA). USENIX, San Jose.

Daneshgar, F., Worasinchai, L., and Low, G., 2011. An Investigation of 'Build vs. Buy'. Decision for Software Acquisition in Small to Medium Enterprises. In: *Conference on Interdisciplinary Business Research*.

Daniel, F., Yu, J., Benatallah, B., Casati, F., Matera, M., Saint-Paul, R., 2007. Understanding UI integration: A survey of Problems, Technologies, and Opportunities. In: IEEEInternet Computi., vol. 11, no. 3, pp.59 -66.

David, P. and Greenstein, S.M., 1990. The Economics of Compatibility Standards: An Introduction to Recent Research," Economics of Innovation and New Technology, Vol. 1, 1990, pp. 1-29.

David, P. A., 1985. Clio and the economics of QWERTY. In: *American Economic Review, Papers and Proceedings, 75*, 332-337.

David, P., 1975. The Landscape and the Machine: Technical Interrelatedness, Land Tenure and the Mechanization of the Corn Harvest in Victorian Britain. In: *Technical Choice, Innovation and Economic Growth*, Cambridge University Press, 1975.

Daylami, N., Ryan, T., Olfman, L. and Shayo, C., 2005. System sciences, *HICSS '05, Proceedings of the 38th Annual Hawaii International Conference*, Island of Hawaii, 3-6 January.

De Filippi P, and McCarthy S., 2012. Cloud Computing: Centralization and Data Sovereignty

de Oliveira, R.R., Martins, R.M. and da Silva Simao, A., 2017. Impact of the Vendor Lock-in Problem on Testing as a Service (TaaS). In *Cloud Engineering (IC2E), 2017 IEEE International Conference on* (pp. 190-196) April. IEEE.

de Villiers, M.R. (2005). Three Approaches as Pillars for Interpretive Information Systems Research: Development Research, Action Research and Grounded Theory. In: Proceedings of the 2005 Annual Research Conference of the South African Institute of Computer Scientists and Information Technologists on IT Research in Developing Countries. SAICSIT '05. [Online]. 2005, Republic of South Africa: South African Institute for Computer Scientists and Information Technologists, pp. 142–151. Available from: http://dl.acm.org/citation.cfm?id=1145675.1145691.

Dell Boomi: The Quest for a Cloud Integration Strategy. Available from: http://www.boomi.com/files/boomi_whitepaper_the_quest_for_cloud_integration_str_ategy_final.pdf [Accessed 8 May 2015].

Dillion, T. Wu, C. and Chang, E., 2010. Cloud Computing: Issues and Challenges, *Advanced Information Networking and Application (AINA). In: 24th IEEE International Conference*, pp. 752-757, 2010.

Di Martino, B. Cretella, G. Esposito, A., 2015. Classification and Positioning of Cloud Definitions and Use Case Scenarios for Portability and Interoperability, in Future Internet of Things and Cloud (FiCloud), 3rd International Conference on, pp.538–544, doi: 10.1109/FiCloud.2015.119

Di Martino, B. Cretella, G. Esposito, A. Sperandeo, R.G., 2014. Semantic Representation of Cloud Services: A Case Study for Microsoft Windows Azure, in Intelligent Networking and Collaborative Systems (INCoS), 2014 International Conference on, pp.647–652, doi: 10.1109/INCoS.2014.76

DMTF, 2012. Distributed Management Task Force. Technical Note. [online].

DPA, 2012. Data Protection Act 1998 - Guidance on the use of cloud computing. [online] Available from: https://ico.org.uk/media/for-organisations/documents/1540/cloud_computing_guidance_for_organisations.pdf [Accessed 1st March 2015].

Dubé JP, Hitsch GJ, Rossi PE., 2009. Do switching costs makes markets less competitive? *Journal of marketing research*, *46*(4), pp.435-445

Dubey, A., and Wagle, D., 2007. Delivering software as a service, The *McKinsey Quarterly* (May), pp. 1–12.

Dutta A, Peng GCA, Choudhary A., 2013. Risks in enterprise cloud computing: the perspective of IT experts. J Comput Inf Syst 53(4):39–48.

Dynamic Market Research, 2013. Cloud for Business Managers. In: Independent Market Research Commissioned by ORACLE (2013). Available from: http://www.qss.ba/doc/2014/?id=794 [13 August 2013].

Ebneter, D., Grivas, S.G., Kumar, T.U., and Wache, H., 2010. Enterprise Architecture Frameworks for Enabling Cloud Computing. In: *3rd IEEE International Conference on Cloud Computing*, pp. 542-543. IEEE Press

Eder, L. and Igbaria, M., 2001. Determinants of intranet diffusion and infusion, *Omega*, Vol. 29 No. 3, pp. 233-242.

Edmonds, A. Metsch, T. Papaspyrou, A. Richardson, A., 2012. Toward an Open Cloud Standard, in Internet Computing, IEEE, vol.16, no.4, pp.15–25 doi: 10.1109/MIC.2012.65

European Network and Information Security Agency (ENISA) 2009a. Cloud Computing: Benefits, risks and recommendations for information security. Available from http://www.enisa.europa.eu/ Accessed 8th February 2015

European Network and Information Security Agency (ENISA) 2009b. Cloud Computing: Information Assurance Framework. Available from http://www.enisa.europa.eu/ [Accessed 8 February 2015].

Farrell, J. Shapiro, C., 1988. Dynamic competition with switching costs. *The RAND Journal of Economics*, pp. 123-137

Farrell, J. Klemperer, P., 2007. Coordination and lock-in: Competition with switching costs and network effects. *Handbook of industrial organization*, *3*, pp. 1967-2072.

Fehling, C., Leymann, F., Mietzner, R. and Schupeck, W., 2011. A Colletion of Patterns for Cloud Types, Cloud Service Models, and Cloud-based Application Architectures. Published by: Insttitue of Architecture of Application Systems (IAAS), Daimler AG. pp. 1-61.

Feng, Y., Li, B. and Li, B., 2014. Price competition in an oligopoly market with multiple IaaS cloud providers. In: *Computers, IEEE Transactions on, vol. 63, no. 1, pp. 59–73*, Jan.

Ferry, N. Hui Song Rossini, A Chauvel, F. Solberg, A., 2014. CloudMF: Applying MDE to Tame the Complexity of Managing Multi-Cloud Applications, in Utility and Cloud Computing (UCC), 2014 IEEE/ACM 7th International Conference on, pp.269–277, doi:10.1109/UCC.2014.36

Fittkau, F., Frey, S. and Hasselbring, W., 2012. CDOSim: Simulating cloud deployment options for software migration support. In *Maintenance and Evolution of Service-Oriented and Cloud-Based Systems (MESOCA), 2012 IEEE 6th International Workshop on the* (pp. 37-46) September. IEEE.

Forrester Research, Inc., 2016. Available from: http://bit.ly/1zDPWxC [Accessed 17 September 2016].

Foster, I., Zhao, Y., Raicu, I. and Lu, S., 2008, November. Cloud computing and grid computing 360-degree compared. In *Grid Computing Environments Workshop, 2008. GCE'08* (pp. 1-10). IEEE.

Fowley, F., Elango, D.M., Magar, H. and Pahl, C., 2017. Software System Migration to Cloud-Native Architectures for SME-Sized Software Vendors. In *International Conference on Current Trends in Theory and Practice of Informatics* (pp. 498-509). Springer, Cham.

Fowler M et al., 2002. Patterns of enterprise application architecture. Addison-Wesley Professional, Reading

Frey, S. and Hasselbring, W., 2010. Model-based migration of legacy software systems to scalable and resource-efficient cloud-based applications: The cloudmig approach.

Frey, S. and Hasselbring, W., 2011. An extensible architecture for detecting violations of a cloud environment's constraints during legacy software system migration. In *Software Maintenance and Reengineering (CSMR), 2011 15th European Conference on* (pp. 269-278) march. IEEE.

Frey, S., Hasselbring, W. and Schnoor, B., 2013. Automatic conformance checking for migrating software systems to cloud infrastructures and platforms. *Journal of Software: Evolution and Process*, *25*(10), pp.1089-1115.

Furht, B, 2010. Handbook of Cloud Computing. Boston: Springer US, 2010, ch. Cloud Comp, pp. 3–19–19. [Online]. Available: http://www.springerlink.com/content/n767118183574r31/ [Accessed 15 July 2016].

Garg, S.K., Versteeg, S. and Buyya, R., 2011. Smicloud: A framework for comparing and ranking cloud services. In *Utility and Cloud Computing (UCC), 2011 Fourth IEEE International Conference on* (pp. 210-218) December. IEEE.

Garg, S.K., Versteeg, S. and Buyya, R., 2013. A framework for ranking of cloud computing services. *Future Generation Computer Systems*, *29*(4), pp.1012-1023.

Gartner Research, 2013. Devising a Cloud Exit Strategy: Proper Planning Prevents Poor Performance. Available from: https://www.gartner.com/doc/2397615/devising-cloud-exit-strategy-proper [Accessed on 7 January 2017].

Gartner, (2016) Hybrid Will Be the Most Common Use of the Cloud [Online]. Available from: http://www.gartner.com/newsroom/id/3354117 [Accessed 14 November 2016]

Gholami, M.F., Daneshgar, F., Low, G. and Beydoun, G., 2016. Cloud migration process—A survey, evaluation framework, and open challenges. *Journal of Systems and Software*, *120*, pp.31-69.

Godse, M. and Mulik, S., 2009, September. An approach for selecting software-as-a-service (SaaS) product. In *Cloud Computing, 2009. CLOUD'09. IEEE International Conference on* (pp. 155-158). IEEE.

Goldkuhl, G., 2011. Pragmatism vs interpretivism in qualitative information systems research. European Journal of Information Systems. [Online]. 21 (2). p.pp. 135– 146. Available from: http://www.palgravejournals.com/doifinder/10.1057/ejis.2011.54.

Gonidis, F. Paraskakis, I. and Kourtesis, D., 2012. Addressing the Challenge of Application Portability in Cloud Platforms. In Proceedings of the 7th South East European Doctoral Student Conference (DSC 2012), pp. 565–576.

Gonidis, F. Simons, A. J. H. Paraskakis, I. and Dimitrios, K., 2013. Cloud application portability: an initial view, p. 275, 2013.

Gonzalez, N., Miers, C., Redigolo, F., Simplico, M. and Carvalho, T., 2012. A Quantitative Analysis of Current Security Concerns and Solutions for Cloud Computing. In: Journal of Cloud Computing: Advances, Systems and Applications, 1:11.

Govindarajan, A. and Lakshmanan, L., 2010. Overview of Cloud Standards, in *Springer Computer Communications and Networks Journal*, London, 2010 pp. 77-89.

Grabova, O., Darmont, J., Chauchat, J. H., and Zolotaryova, I., 2010. Business intelligence for Small and Middle-sized Enterprises'. *SIGMOD Record, 39(2)*, 39-50.

Green, J. & Browne, J., 2005. Principles of social research. Maidenhead: Oxford university press.

Greschler, D., Mangan, T., 2002. Networking lessons in delivering 'Software as a Service': part II, International Journal of Network Management, Volume 12 Issue 6, John Wiley & Sons Inc., November 2002, pp. 317-321.

Guzzo, R.A., S.E. Jackson, and R.A., Katzell, 1987. Meta-analysis Analysis, Research in Organizational Behavior (9), pp. 407–442

Gunther, S., Haupt, M., and Splieth, M., 2010. Utilizing Internal Domain-Specific Languages for Deployment and Maintenance of IT Infrastructures. Technical report, Very Large Business Applications Lab Magdeburg, Fakultat fur Informatik, Otto-von-Guericke-Universitat Magdeburg

Hair, JF, Anderson, RE, Tatham, RL, Black, WC., 1992. Multivariate Data Analysis, 3rd edn. Macmillan, New York

Hajjat, M., Sun, X., Sung, Y., Maltz, D., Rao, S., Sripanidkulchai, K., Tawarmalani, M.: Cloudward bound: planning for beneficial migration of enterprise applications to the cloud. In: ACM SIGCOMM Computer Communication Review. vol. 40, pp. 243–254. ACM (2010)

Harsh, P., Dudouet, F., Cascella, R. G., J´egou, Y., and Morin, C., 2012. Using Open Standards for Interoperability - Issues, Solutions, and Challenges facing Cloud Computing. arXiv.org, vol. cs.DC, Jul.

Herbert L, 2013. Forrester SaaS Capabilities Maturity Assessment. Forrester Research [online]. Available from: http://media.cms.bmc.com/documents/Forrester_SaaS_Capabilities_Maturitity_Assessment+(2).pdf [Accessed 5 January 2017].

Hoberg, P. Wollersheim, J. & Krcmar, H., 2012. The business perspective on Cloud Computing: A literature review of research on Cloud Computing. In Proceedings of the AMCIS.

Hofmann P. and Woods, D. Cloud Computing: The Limits of Public Clouds for Business Applications, IEEE Internet Computing, vol. 14, no. 6, pp. 90–93, Nov. 2010.

Hogan, M. Liu, F. Sokol, A. and Tong, J., 2011. NIST Cloud Computing Standards Roadmap, *NIST Special Publication* 500-291, July [online]. Available from: http://www.nist.gov/itl/cloud/upload/NIST_SP-500-291_Jul5A.pdf [Accessed 7th January 2015].

Hoover, J. N., & Martin, R., 2008. Demystifying the Cloud: Information Week Research & Reports [online]. Available from: [Accessed on 2 July 2014].

Horrocks, I., Patel-Schneider, P.F., Boley, H., Tabet, S., Grosof, B. and Dean, M., 2004. SWRL: A semantic web rule language combining OWL and RuleML. *W3C Member submission*, *21*, p.79.

Hintsch, J., Schrödl, H., Scheruhn, H.J., Turowski, K., Thomas, O. and Teuteberg, F., 2015. Industrialization in Cloud Computing with Enterprise Systems: Order-to-Cash Automation for SaaS Products. In *Wirtschaftsinformatik* (pp. 61-75).

Hudli, A. V. Shivaradhya, B. and Hudli, R.V., 2009. Level-4 SaaS applications for healthcare industry," COMPUTE '09: Proceedings of the 2nd Bangalore Annual Compute Conference, Proceedings of ACM, January.

Humble J. and Farley D., 2010. Continuous Delivery: Reliable Software Releases through Build, Test, and Deployment Automation. Addison-Wesley Professional.

Hummer, W, Rosenberg, F., Oliveira, F and Eilam, T., 2013. Automated testing of chef automation script. In: Proceedings of ACM/IFIP/USENIX 14th International Middleware Conference

Hwang, M.I., and Thorn, R.G., 1999. The Effect of User Engagement on System Success: A Meta-Analytical Integration of Research Findings, Information & Management (35), pp. 229–236.

Hwang, K., and Li, D., 2010. Trusted Cloud Computing with Secure Resources and Data Colouring, IEEE Internet Computing (14)5, p. 14.

Iannucci, P., Gupta, M., et al., 2013. IBM SmartCloud: Building a Cloud Enabled Data Center. IBM Redbooks, New York.

IBM, 2012. Successful Information Governance through High-quality Data. In: *IBM Software Whitepaper*, Information Management.

ICO, 2012. Information Commissioner's Office. Anonymisation: managing data protection risk code of practice, ICO, November.

IDC, Cloud computing 2010 – an IDC update, 2010. [online] Available from: http://www.cionet.com/Data/files/groups/Cloud%20Computing%202010%20-%20An%20IDC%20Update.pdf [Accessed 12th January 2015].

Informatica Whitepaper, 2010. Cloud Integration for Hybrid IT – Balancing Business SelfService and IT Control, whitepaper.

Iyer, B., & Henderson, J. C., 2010. Preparing for the future— understanding the seven capabilities of Cloud Computing. MIS Quarterly Executive (pp. 117–131).

Izza, S., 2009. Integration of industrial information systems: From syntactic to semantic integration approaches. In: Enterprise Inform. Syst., vol. 3, no. 1, pp.1 -57.

Jammal, M., Singh, T., Shami, A., Asal, R. and Li, Y., 2014. Software defined networking: State of the art and research challenges. *Computer Networks*, *72*, pp.74-98.

Jamshidi, P. Ahmad, A. and Pahl, C., 2013. Cloud Migration Research: A Systematic Review" IEEE Transactions on Cloud Computing. Available from: http://doras.dcu.ie/19636/1/TCC-AcceptedVersion.pdf [Accessed on the 5 March 2014].

Jamshidi, P., Pahl, C., Chinenyeze, S. and Liu, X., 2015. Cloud migration patterns: a multi-cloud service architecture perspective. In *Service-Oriented Computing-ICSOC 2014 Workshops* (pp. 6-19). Springer International Publishing.

Jansen, W. and Grance, T., 2011. Sp 800-144. guidelines on security and privacy in public cloud computing.

Janssen, M. and Joha, A., 2011. Challenges for adopting cloud-based software as a service (saas) in the public sector. In *ECIS*.

Jha, A.K., DesRoches, C.M., Campbell, E.G., Donelan, K., Rao, S.R., Ferris, T.G., Shields, A., Rosenbaum, S. and Blumenthal, D., 2009. Use of electronic health records in US hospitals. *New England Journal of Medicine*, *360*(16), pp.1628-1638.

JISC Legal Information, 2011. Report on Cloud Computing and the Law for UK FE and HE (An Overview).

Joshi, S., 2009. Architecture for SaaS Applications–Using the Oracle SaaS Platform. Oracle White Chapter.

Joshi, K.P., Yesha, Y, Finin, T., 2014. Automating Cloud Services Life Cycle through Semantic Technologies. *J. IEEE Transactions on Services Computing*, Vol. 7 (1), 109-122 (2014).

Kächele, S., Spann, C., Hauck, F.J. and Domaschka, J., 2013, December. Beyond IaaS and PaaS: An extended cloud taxonomy for computation, storage and networking. In *Proceedings of the 2013 IEEE/ACM 6th International Conference on Utility and Cloud Computing* (pp. 75-82). IEEE Computer Society.

Kaisler, S., Money, W. H., & Cohen, S. J., 2012. A decision framework for Cloud Computing. In Proceedings of the HICSS (pp. 1553–1562). IEEE

Kalloniatis, C., Mouratidis, H., Vassilis, M., Islam, S., Gritzalis, S. and Kavakli, E., 2014. Towards the design of secure and privacy-oriented information systems in the cloud: Identifying the major concepts. *Computer Standards & Interfaces*, *36*(4), pp.759-775.

Kaplan, B.B.B. & Duchon, D., 1988. Combining Qualitative and Quantitative Methods in Information Systems Research: A Case Study. MIS Quarterly. [Online]. 12 (4). p.pp. 571–586. Available from: http://search.ebscohost.com/login.aspx?direct=true&db=bth&AN=4679634&lang =es&site=ehost-live

Kavis, M., 2014. Architecting the Cloud: Design Decisions for Cloud Computing Service Models (SaaS, PaaS, and IaaS), John Wiley & Sons.

Keele, S. Guidelines for performing systematic literature reviews in software engineering. In Technical report, Ver 2.3 EBSE Technical Report. EBSE. Sn.

Khanapurkar, N., 2011. The Cloud: Changing the Business Ecosystem. [online] Available from:: http://www.kpmg.com/IN/en/IssuesAndInsights/ThoughtLeadership/The _Cloud_Changing_the_Business_Ecosystem.pdf [Accessed 10 November 2014].

Khajeh-Hosseini, A., Greenwood, D. and Sommerville, I., 2010. Cloud migration: A case study of migrating an enterprise it system to iaas. In *Cloud Computing (CLOUD), 2010 IEEE 3rd International Conference on* (pp. 450-457) july. IEEE.

Khajeh-Hosseini, A. Sommerville, I. and Sriram, I., 2010. Research challenges for enterprise cloud computing," Information Security, no. 1960.

Khajeh-Hosseini A, Greenwood D, Smith JW, Sommerville, I., 2012. The Cloud Adoption Toolkit: Supporting Cloud Adoption Decisions in the Enterprise. *Software: Practice and Experience*, vol. 42 (4), pp. 447–465

Kitchenham, B., 2004. In: Procedures for Undertaking Systematic Reviews. Joint Technical Report, Computer Science Department, Keele University (TR/SE-0401) and National ICT Australia Ltd (0400011T.1).

King, I., 2014. Cloud Spending by Companies Outpaces Predictions, Forrester Says [Online]. Available from: https://www.bloomberg.com/news/articles/2014-04-24/cloud-spending-by-companies-outpaces-predictions-forrester-says [Accessed 7 November 2016]

Klein, H. & Myers, M., 2011. A Set of Principles for Conducting Critical Research in Information Systems. MIS Quarterly. [Online]. 35 (1). p.pp. 17–36. Available from: http://misq.org/a-set-of-principles-for-conducting-critical-research-ininformation-systems.html. Accessed 8th September 2015.

Klemperer, P., 1987. Markets with consumer switching costs. *The quarterly journal of economics*, *102*(2), pp. 375-394.

Klemperer P., 1987. The competitiveness of markets with switching costs. *The RAND Journal of Economics*, pp. 138-150.

Klemperer P., 1989. Price wars caused by switching costs. *The Review of Economic Studies*, *56*(3), pp. 405-420

KPMG, 2013. Breaking through the Cloud Adoption Barriers, *Cloud Providers Survey* [online] https://www.kpmg.com/LU/en/IssuesAndInsights/Articlespublications/Documents/breaking-through-the-cloud-adoption-barriers.pdf [Accessed 24 November 2014].

Kratzke, N., 2014. Lightweight virtualization cluster how to overcome cloud vendor lock-in. *Journal of Computer and Communications*, *2*(12), p.1.

Kurze, T., Klems, M., Bermbach, D., Lenk, A., Tai, S. and Kunze, M., 2011. Cloud federation. In *Proceedings of the 2nd International Conference on Cloud Computing, GRIDs, and Virtualization (CLOUD COMPUTING 2011)* (Vol. 1971548541).

Laplante, P.A., Zhang, J. and Voas, J., 2008. What's in a Name? Distinguishing between SaaS and SOA. *It Professional*, *10*(3).

Laszewski, T. and Nauduri, P., 2011. *Migrating to the cloud: Oracle client/server modernization*. Elsevier.

Leimbach T., Hallinan, D., Bachlechner, D., Weber, A., Jaglo, M., Hennen, L., Nielsen, R.O., Nentwich, M., StrauB, S., Lynn, T. and Hunt, G., 2014. Potential and Impacts of Cloud Computing Services and Social Network Websites, *Publication of Science and Technology Options Assessment*, [online] http://www.europarl.europa.eu/RegData/etudes/etudes/join/2014/513546/IPOL-JOIN_ET(2014)513546_EN.pdf [Accessed 14 November 2014].

León, X., Chaabouni, R., Sánchez-Artigas, M., Garcia-Lopez, P., 2014. Transparently integrating BitTorrent in the data center with smart cloud seeding. IEEE Internet Computing. 18, 47– 54.

Lewis, G. A., 2012. Role of Standards in Cloud-Computing Interoperability. In: *IEEE, 46th Hawaii International Conference on System Sciences*, pp. 1652-1661.

Leymann, F., 2009. Cloud Computing: The Next Revolution in IT. [online] Available from: http://www.ifb.uni-stuggart.de/publications/phowo09/010Leymann.pdf [Accessed on 12 November 2014].

Leymann F et al., 2011. Moving Applications to the Cloud: An Approach Based on Application Model Enrichment. Int'l J Cooperative Information Systems 20(3):307–356

Liao, H. and Tao, C., 2008. An Anatomy to SaaS Business Mode Based on Internet, ICMECG, 2008 International Conference on Management of eCommerce and e-Government, pp.215-220.

Lindner, M., McDonald, F., Conway, G. and Curry, E., 2011. Understanding cloud requirements-a supply chain lifecycle approach. In *Proceedings of the Second International Conference on Cloud Computing, GRIDs, and Virtualization CLOUD COMPUTING 2011*. XPS (Xpert Publishing Services).

Lipton, P., 2013. Escaping Vendor Lock-in with TOSCA, an Emerging Cloud Standard for Portability, *In: CA Technology Exchange* 4, 1.

Liu, X. and Ye, H., 2008. A Sustainable Service-Oriented B2C Framework for Small Businesses', *4th IEEE International Symposium on Service Oriented Systems Engineering* (SOSE'08), Taiwan, December.

Liu, F., Tong, J., Mao, J., Bohn, R., Messina, J., Badger, L. and Leaf, D., 2011. NIST Cloud Computing Reference Architecture. *NIST Special Publication*, *500*, p.292.

Lloyd, W., Pallickara, S., David, O., Lyon, J., Arabi, M. and Rojas, K., 2011, September. Migration of multi-tier applications to infrastructure-as-a-service clouds: An investigation using kernel-based virtual machines. In *Grid Computing (GRID), 2011 12th IEEE/ACM International Conference on* (pp. 137-144). IEEE.

Loutas, N., Peristeras, V., Bouras, T., Kamateri, E., Zeginis, D., and Tarabanis, K., 2010. Towards a Reference Architecture for Semantically Interoperable Clouds, *in IEEE Second International Conference on Cloud Computing Technology and Science*, , pp. 143-150.

Loutas, N., Kamateri, E., Bosi, F., and Tarabanis, K.A., 2011. Cloud Computing Interoperability: The State of Play, *In CloudCom*, pp. 752–757.

Ma D, Kauffman RJ., 2014. Competition between software-as-a-service vendors. *IEEE Transactions on Engineering Management*, *61*(4), pp.717-729

Machado, G. S. Hausheer, D. and Stiller B., 2010. Considerations on the Interoperability of and between Cloud Computing Standards [online]. Available from: http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.155.51 [Accessed on 20th May 2016].

Marks, A.E. and Lozano, B. 2010. *Executive's Guide to Cloud Computing.* John Wiley & Sons, eBook.

Marston, S., Li, Z., Bandyopadhyay, S., Zhang, J. and Ghalsasi, A., 2011. Cloud computing—The business perspective. Decision support systems, 51(1), pp.176-189.

Mahmood, Z., Hill, R. 2011. Cloud Computing for Enterprise Architectures. SpringerVerlag, London.

Mann, V., Vishnoi, A., Kannan, K., Kalyanaraman, S., 2012. CrossRoads: Seamless VM Mobility across Data Centers through Software-Defined Networking, 2012 IEEE Network Operations and Management Symposium (NOMS), pp.88–96, 16–20 April.

Martino, B., Petcu, D., Cossu, R., Goncalves, P., Mhr, T., and Loichate M., 2011. Building a mosaic of clouds. Lecture Notes in Computer Science. In Euro-Par 2010 Parallel Processing Workshops.Eds. Springer Berlin Heidelberg, vol. 6586, pp. 571, –578. [Online]. Available: http://dx.doi.org/10.1007/978-3-642-21878-1_70

Martino, B., Cretella, G. and Esposito, A., 2015. Cloud Portability and Interoperability Issues and Current Trends, IN: *Springer Briefs in Computer Science*.

Mell, P. and Grance, T., 2009. The NIST Definition of Cloud Computing, *Technical report*.

Mell, P., & Grance, T., 2011. The NIST Definition of Cloud Computing (Draft): Recommendations of the National Institute of Standard and Technology. Available from: http://csrc.nist.gov/publications/drafts/800-145/Draft-SP-800-145_cloud-definition.pdf [Accessed 2 August 2014].

Menychtas, A., Santzaridou, C., Kousiouris, G., Varvarrigou, T., Orue-Echevarria, L., Alonso, J., Gorronogoitia, J., Bruneliere, H., Strauss, O., Senkova, T., Pellens, B., Steur, P., 2013. ARTIST Methodology and Framework. A Novel approach for migration of Legacy Software on the Cloud. In:

2013 15th International Symposium on Symbolic and Numeric Algorithms for Scientific Computing (SYNASC), pp. 424-431. Doi:10.1109/SYNASC.2013.62

Menzel, M. and Ranjan, R., 2012. CloudGenius: decision support for web server cloud migration. In *Proceedings of the 21st international conference on World Wide Web* (pp. 979-988). ACM.

Michael A, Armando F, Rean G, Anthony DJ, Randy HK, Andrew K, Gunho L, David AP, Ariel R, Ion S, Matei Z (2010) A view of cloud computing. Commun ACM 53(4):50–58

Mietzner, R., Papazoglou, M.P. and Leymann, F., 2008. Defining Composite Configurable SaaS application packages using SCA, variability descriptors and multi-tenancy patterns. [Online].

Mimecast, 2010. Cloud Computing Adoption Survey [online]. Availabe from http://www.mimecast.com [Accessed 8 February 2015].

Mingers, J., 2003. The paucity of multimethod research: a review of the information systems literature. Information Systems Journal [online]. 13 (3). p.pp. 233–249. Available from: http://onlinelibrary.wiley.com/doi/10.1046/j.1365- 2575.2003.00143.x/full.

Miranda, J. Guillen, J. and Murillo, J., 2012. Identifying Adaptation Needs to Avoid the Vendor Lock-in Effect in the Deployment of Cloud ServiceBased Applications (SBAs), *WAS4FI I-Mashups September 19 Bertinoro*, Italy.

Miranda, J., Guilléen, J., Murillo, J. M. and Canal, C., 2012. Enough about Standardization, Let's Build Cloud Applications. In: Nordicloud Workshop at WICSA/ECSA'12, p. 4.

Miranda, J., Guillen, J., Murillo, J.M., and Canal, C., 2013. Assisting Cloud Service Migration Using Software Adaptation Techniques. In: 2013 IEEE Sixth International Conference on Cloud Computing (CLOUD), vol., no., pp.573,580, June 28 2013-July 3 2013 doi: 10.1109/CLOUD.2013.3

Mircea, M. and Andreescu, A.I., 2011. Using cloud computing in higher education: A strategy to improve agility in the current financial crisis. *Communications of the IBIMA*.

Mohagheghi, P., Berre, A.J., Sadovykh, A., Barbier, F., Benguria, G., 2010. Reuse and Migration of Legacy Systems to Interoperable Cloud Services-the REMICS project. In: Proceedings of Mda4Service Cloud.

Mohagheghi, P. and Sther, T., 2011. Software Engineering Challenges for Migration to the Service cloud Paradigm: On-going work in the Remics project, in Services (SERVICES), 2011 IEEE World Congress on, July 2011, pp. 507– 514.

Mohamed, A., 2009. A History of Cloud Computing. Available from: utilitycomputing.com/links/AHistoryOfCloudComputing20090327.asp [Accessed on 2nd July 2014].

Myers, M. & Avison, D., 2002. Qualitative research in information systems: a reader. [Online]. London: SAGE. Available from: http://books.google.com/books?hl=en&lr=&id=Oe9jkjrdFuoC&oi=fnd&pg=PP2 &dq=Qualitative+research+in+information+systems:+a+reader&ots=QEvYSkXF 8k&sig=QZeRZRuS9q-IpyG8Kb54W59n3V0.

Nitto, E.D., Silva, M.A.A.D., Ardagna, D., Casale, G., Craciun, C.D., Ferry, N., Muntes, V., Solberg, A., 2013. Supporting the Development of and Operation of Multi-Cloud Applications, the

MODAClouds Approach. IN: 15th International Symposium on Symbolic and Numeric Algorithms for Scientific Computing (SYNASC), pp. 417-423. doi: 10.1109/SYNASC.2013.61

Nelson-Smith, S., 2011. Test-Driven Infrastructure with Chef. O'Reilly.

Nelson V. and Uma, V., 2012. Semantic based Resource Provisioning and scheduling in inter-cloud environment, in International Conference on Recent Trends in Information Technology, 2012, pp. 250–254.

Nitu, 2009. Configurability in SaaS (software as a service) applications ISEC '09: Proceeding of the 2nd annual conference on India software engineering conference, February 2009, pp. 19-26.

Nielsen, J. and Levy, J., 1994. Measuring usability: preference vs. performance." Communications of the ACM, 37(4):66–75, Apr. 1994.

Notkin, D., Black, A.P., Lazowska, E.D., Levy, H.M., Sanislo, J. and Zahorjan, J., 1988. Interconnecting heterogeneous computer systems. *Communications of the ACM*, *31*(3), pp.258-273.

Nurmi, D. Wolski, R. Grzegorczyk, C. Obertelli, G. Soman, S. Youseff, L. and Zagorodnov, D., 2009. The Eucalyptus Open-Source Cloud-Computing System, Proc. of IEEE International Symposium on Cluster Computing and the Grid (CCGrid).

Nussbaumer, N., and Liu, X., 2013. Cloud Migration for SMEs in a Service Oriented Approach. In: *IEEE 37th Annual Computer Software and Applications Conference Workshops (COMPSACW).* pp. 457-462.

NVivo qualitative data analysis software; QSR International Pty Ltd. Version 8, 2008.

OASIS, 2007. Web Services Business Process Execution Language (BPEL) Version 2.0Google Scholar

OASIS Cloud Application Management for Platforms, version 1.0., 2012. Available from: https://www.oasis-open.org/committees/download.php/47278/CAMP-v1.0.pdf

OASIS Topology and Orchestration Specification for Cloud Applications (TOSCA) Version 1.0, Committee Specification Draft 04 (2012).

OASIS UDDI Specification, 2016. [online]. Available from: http://www.oasisopen.org/committees/uddispec/doc/tcspecs.htm [Accessed on 5 March 2016].

Oates, B., 2005. Researching information systems and computing [online]. Available from: http://books.google.com/books?hl=en&lr=&id=VyYmkaTtRKcC&oi=fnd&pg=PR11&dq=researching+information+systems+and+computing&ots=w7_AwXLMZE&sig=S3NwER2Lk21zZKlpT_3a0Ig5sU4 [Accessed on 24 October 2015].

Oltsik, J., Laliberte, B., 2012. IBM and NEC Bring SDN/OpenFlow to Enterprise Data Center Networks, Enterprise Strategy Group Tech Brief.

Ooi S.L., Su, M.T., 2006. Integrating Enterprise Application using Message-oriented Middleware and J2EE Technologies. In: Proc.Int. Conf. Comput. Informat., pp.1 -5.

Opara-Martins, J., Sahandi, R., and Tian, F., 2014. Critical review of vendor lock-in and its impact on adoption of cloud computing, *International Conference on Information Society (i-Society)*, vol., no., pp.92,97, 10-12 Nov. doi: 10.1109/i-Society.2014.7009018

Opara-Martins J, Sahandi R, Tian F., 2015a. Implications of integration and interoperability for enterprise cloud-based applications. In *International Conference on Cloud Computing* (pp. 213-223). Springer International Publishing.

Opara-Martins J, Sahandi R, Tian F., 2015b. A Business Analysis of Cloud Computing: Data Security and Contract Lock-in Issues. In *P2P, Parallel, Grid, Cloud and Internet Computing (3PGCIC), 2015 10th International Conference on*, pp. 665-670 November. IEEE

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), pp. 1-18

OpenTOSCA, 2015. Available from: http://www.iaas.uni-stuttgart.de/OpenTOSCA [Accessed on 24 October 2015].

The Open Group, 2011. SOA Reference Architecture Technical Standard: Integration Layer. In: SOA Source Book, (2011). Available from: https://www.opengroup.org/soa/source-book/soa_refarch/integration.htm [Accessed on 26 May 2014].

The OpenGroup Consortium. Available from: http://www.opengroup.org [Accessed on 26 May 2014].

OpenStack Foundation, 2016 [online]. Available from: http://bit.ly/WRAGiU [Accessed 17th September 2016]

Oracle, 2009. Architectural Strategies for Cloud Computing, in Oracle White Paper in Enterprise Architectures, August.

Orellana, J.P., Caminero, M.B. and Carrión, C., 2014, December. On the provision of SaaS-level quality of service within heterogeneous private clouds. In *Utility and Cloud Computing (UCC), 2014 IEEE/ACM 7th International Conference on* (pp. 146-155). IEEE.

OVF, 2008. Distributed Management Task Force OVF. Overview Document. [online].

Pahl, C., Xiong, H. and Walshe, R., 2013. A comparison of on-premise to cloud migration approaches. In *European Conference on Service-Oriented and Cloud Computing* (pp. 212-226). Springer Berlin Heidelberg.

Pardo, J., Flavin, A. and Rose, M., 2016. 2016 Top Markets Report - Cloud Computig [Online]. Available from: http://www.trade.gov/topmarkets/pdf/Cloud_Computing_United_Kingdom.pdf Accessed on 7th November 2016.

Parameswaran, A.V. and Chaddha, A., 2009. Cloud Interoperability and Standardization, *Infosys, SETLabs Briefings*, 7(7):19–26.

Peddigari, B.P., 2011. Unified Cloud Migration Framework - Using factory based approach. India Conference (INDICON), 1-5.

Peng, H.T., Hsu, W.W., Chen, C.H., Lai, F. and Ho, J.M., 2013, September. FinancialCloud: Open cloud framework of derivative pricing. In *Social Computing (SocialCom), 2013 International Conference on* (pp. 782-789). IEEE.

Petcu, D., Craciun, C. and Rak, M., 2011. Towards a cross platform cloud API. In *1st International Conference on Cloud Computing and Services Science* (pp. 166-169).

Petcu, D., 2011. Portability and interoperability between clouds: Challenges and case study. In: *Towards a Service-Based Internet, vol. 6994 LNCS*,

Petcu D, Macariu G, Panic S, Craciun C (2013) Portable cloud applications- from theory to practice. Futur Gener Comput Syst 29(6):1417–1430, https://doi.org/10.1016/j.future.2012.01.009

Petcu, D. and Vasilakos, A.V., 2014. Portability in clouds: approaches and research opportunities, *Scalable Computing: Practice and Experience*, Volume 15, Issue 3, Sept, pp. 251-270.

Petcu D, Vasilakos AV., 2014. Portability in clouds: approaches and research opportunities. Scalable Comput Practice Experience 15(3):251–270.

Petter, S., and E.R. McLean 2009. A Meta-Analytic Assessment of the Delone and Mclean IS Success Model: An Examination of IS Success at the Individual Level, Information & Management (46)3, pp. 159–166.

Petticrew, M. and Roberts H., 2005. Systematic Reviews in the Social Sciences: A Practical Guide, Blackwell Publishing, 2005, ISBN 1405121106

Polikaitis A, 2015. Vendor and Sourcing Management: Maintaining Control of Vendor Relationships by Avoiding Vendor Lock-in. IDC Opinion Report. http://core0.staticworld.net/assets/2016/04/19/idc-vsmavoiding-vendor-lock-in.pdf. [Accessed 12 November 2016].

Pooyan, J. Aakash, A. and Claus, P., 2013. Cloud Migration Research: A Systematic Review, *IEEE Transactions on Cloud Computing*, [online]. Available from: http://doras.dcu.ie/19636/

Premkumar, G. and Michael, P., 1995. Adoption of computer aided software engineering (CASE) technology: an innovation adoption perspective', *SIGMIS Database*, Vol. 26 No 2-3, pp. 105-124.

Pritzker, P. and Gallagher, D. P., 2013. NIST Cloud Computing Standards Roadmap. *NIST Special Publication 500-291, Version 2* [online]. Available from: http://collaborate.nist.gov/twiki-cloud-computing/pub/CloudComputing/StandardsRoadmap/NIST_SP_500-291_Version_2_2013_June18_FINAL.pdf [Accessed on 15th July 2016].

PrudHommeaux, E., Seaborne, A., et al., 2008. SPARQL Query Language for RDF. W3C Recommendation 15.

Puppet Labs, 2015. Open Source Puppet. Available from https://puppetlabs.com/puppet/puppet-open-source [Accessed 28 February 2016].

Rackspace US, Inc., http://bit.ly/1pvVnKC [Accessed 17 September 2016].

Rafique, A., Walraven, S., Lagaisse, B., Desair, T. and Joosen, W., 2014. Towards portability and interoperability support in middleware for hybrid clouds. In *Computer Communications Workshops (INFOCOM WKSHPS), 2014 IEEE Conference on* (pp. 7-12). IEEE.

Rai, R., Sahoo, G. and Mehfuz, S., 2015. Exploring the factors influencing the cloud computing adoption: a systematic study on cloud migration. *SpringerPlus*, *4*(1), p.197.

Raj, P. and Periasamy, M., 2011. The Cloud Challenges for Enterprise Architectures. In: Computer Communications and Networks, Springer-Verlag London Limited, 2011. DOI 10.1007/978-1-4471-2236-4_10

Raj, P., 2013. Cloud Enterprise Architecture. Taylor and Francis Group, USA. pp. 21-29.

Razavian, S. M., Khani, H. and Yazdani, N., 2013. An Analysis of Vendor Lock-in Problem in Cloud Storage. In: 3rd International Conference on Computer Knowledge Engineering (ICCKE).

Rehman, Z., Hussain, F.K. and Hussain, O.K., 2011, June. Towards multi-criteria cloud service selection. In *Innovative Mobile and Internet Services in Ubiquitous Computing (IMIS), 2011 Fifth International Conference on* (pp. 44-48). IEEE.

Rittinghouse, W. J., & Ransome, F. J., 2010. Cloud Computing: Implementation, Management and Security.

Robey, D. and Markus, M.L., 1997. Beyond Rigor and Relevance: Producing Consumable Research About Information Systems, Information Resources Management Journal.

Rochwerger, B., Breitgand, D., Levy, E., Galis, A., Nagin, K., Llorente, I. M., and Galan, F., 2009. The reservoir model and architecture for open federated cloud computing, *IBM Journal of Research and Development*, 53(4), 4-1.

Rodero-Merino, L., Vaquero, L.M., Gil, V., Galán, F., Fontán, J., Montero, R.S., and Llorente, I.M. 2010. From infrastructure delivery to service management in clouds, *Future Generation Computer Systems*, vol. 26, no. 8, pp. 1226-1240.

Rosenberg, F., Leitner, P., Michlmayr, A., Celikovic, P. And Dustdar, S., 2009. Towards Composition as a Service – A Quality of Service Driven Approach. [online] Available from: http://ieeexplore.org/Ipdocs/epic03/wrapper.htm?arnumber=4812599 [Accessed 28 October 2014].

RunMyProcess, 2015. Workflow Builder [online]. Available from: http://www.runmyprocess.com [Accessed 17 September 2016].

Ruby, 2016. Available from: https://www.ruby-lang.org/en/ [Accessed 17 September 2016]

Sabherwal, R., A. Jeyaraj, and C. Chowa, 2006. Information System Success: Individual and Organizational Determinants, Management Science (52)12, p. 1849.

Sabharwal N, Wadhwa M., 2014. Automation through Chef Opscode: A Hands-on Approach to Chef

Sahandi R, Alkhalil A, Opara-Martins, J., 2012. SMEs' perception of cloud computing: Potential and security. In *Working Conference on Virtual Enterprises* (pp. 186-195) October. Springer Berlin Heidelberg

Sahandi, R., Alkhalil, A. and Opara-Martins, J., 2013. Cloud Computing from SMEs Perspective: A Survey Based Investigation, *Journal of Information Technology Management*, A Publication of the Association of Management, vol. XXIV (1), pp. 1-12. ISSN #1042-1319.

Sampaio A.and Mendonça, N., 2011. “Uni4Cloud,” in 2nd Intl. workshop on Software engineering for cloud computing, pp. 15–21

Sanaei, Z., Abolfazli, S., Gani, A. and Buyya, R., 2014. Heterogeneity in mobile cloud computing: taxonomy and open challenges. *IEEE Communications Surveys & Tutorials*, *16*(1), pp.369-392.

Sarna, E.V. D., 2011. Implementing and Developing Cloud Computing Applications. Taylor and Francis Group, USA.

Satzger, B. Hummer, W. Inzinger, C. Leitner, P. and Dustdar, S., 2013. Winds of Change: From Vendor Lock-In to the Meta Cloud. In: IEEE Internet Computing, vol. 17, no. 1, pp. 69–73, Jan. 2013.

Schroeter, J. Cech, S. G¨otz, S. Wilke, C.and Aßmann U., 2012a. Towards modeling a variable architecture for multi-tenant saas-applications. In Proceedings of the sixth International Workshop on Variability Modelling of Software-Intensive Systems (VaMoS ’12), pages 111–120. ACM.

Schroeter, J., Mucha, P., Muth, M., Jugel, K. and Lochau, M., 2012b. Dynamic configuration management of cloud-based applications. In *Proceedings of the 16th International Software Product Line Conference-Volume 2* (pp. 171-178). ACM.

Schubert, L. Jeffery, K. and Neidecker-Lutz, B., 2010. The future of cloud computing,” European Commission - Information Society and Media, Tech. Rep., 2010.

Shan, C., Heng, C., and Xianjun, Z., 2012. Inter-cloud operations via NGSON, *IEEE Communications Magazine*, vol. 50, no. 1, pp. 82–89, January.

Sherif, M., & Sherif, C. W., 1967. Attitude, ego, involvement and change. New York: John Wiley and Sons Inc.

Sheth. A. and Ranabahu, A., 2010. Semantic Modelling for Cloud Computing, Part I & II. IEEE Internet Computing Magazine, vol. 14, pp. 81-83.

Shin J, Sudhir K., 2008. *Switching costs and market competitiveness: De-constructing the relationship*.Working Paper. Retrieved from http://faculty.som.yale.edu/ksudhir/papers/Switching% 20Cost Shin% 20and%20Sudhir% 202008.pdf

Silva, G. C., Rose, L. M., and Calinescu., 2013. A Systematic Review of Cloud Lock-in Solutions. In 5th IEEE International Conference on Cloud Computing Technology and Science.

Silva, G. C., Rose, L. M., Calinescu, R., 2013. Towards a Model-Driven Solution to the Vendor Lock-In Problem in Cloud Computing. In: IEEE 5th International Conference on Cloud Computing Technology and Science (CloudCom), vol.1, no., pp.711,716, 2-5 Dec. doi: 10.1109/CloudCom.2013.131

Silverman, D., 1998. Qualitative research: meanings or practices? Information Systems 252 Journal. [Online]. 8 (1). p.pp. 3–20. Available from: http://doi.wiley.com/10.1046/j.1365-2575.1998.00002.x.

Sitaram, D and Manjunath, G., 2012. Moving to the Cloud: Developing Apps in the New World of Cloud Computing. *Elsevier*, USA.

Simple Object Access Protocol (SOAP), [online]. Available from http://www.w3.org/tr/soap/, [Accessed 17 September 2015].

Sosinksy, B., 2011. Cloud Computing Bible. John Wiley and Sons.

Spinellis, D., 2012. Don't Install Software by Hand. IEEE Software. 29, 86–87

Spinola, M., 2009. An Essential Guide to Possibilities and Risks of Cloud Computing. Available from: [Accessed on 2nd July 2011].

Srinivasan, M.K., Sarukesi, K., Rodrigues, P., Manoj, M.S. and Revathy, P., 2012, August. State-of-the-art cloud computing security taxonomies: a classification of security challenges in the present cloud computing environment. In *Proceedings of the international conference on advances in computing, communications and informatics* (pp. 470-476). ACM.

Srivastava, V., Bond, M.D., McKinley, K.S. and Shmatikov, V., 2011. A security policy oracle: Detecting security holes using multiple API implementations. *ACM SIGPLAN Notices*, *46*(6), pp.343-354.

Stifani, R., Pappe, S., Brieter, G. and Behrendt, M. 2012. IBM Cloud Computing Reference Architecture [online]. Available from: http://www-05.ibm.com/it/cloud/downloads/Cloud_Computing.pdf [Accessed 25 May 2016].

Strauch, S., Andrikopoulos, V. and Bachmann, T., 2013. Migrating application data to the cloud using cloud data. In *e 3rd International Conference on Cloud Computing and Service Science, (CLOSER)* (pp. 36-46).

Stravoskoufos, K., Preventis, A., Sotiriadis, S. and Petrakis, E.G., 2014. A Survey on Approaches for Interoperability and Portability of Cloud Computing Services. In *CLOSER* (pp. 112-117).

Sultan, N. A., 2011. Reaching for the "cloud": How SMEs can manage. *International Journal of Information Management*, *31(3)*, 272–278.

Survey Monkey, 2014. Online Survey Development Tool [online]. Available from: https://www.surveymonkey.com [Accessed 17 September 2014].

SnapLogic and TechValidate: Cloud Integration Drivers and Requirements (survey) in 2015[online]. Available from: http://campaigns.snaplogic.com/rs/snaplogic/images/cloudintegration-drivers-and-requirements-in-2015.pdf [Accessed 24 May 2015].

Takabi, H., Joshi, J.B. and Ahn, G.J., 2010. Security and privacy challenges in cloud computing environments. *IEEE Security & Privacy*, *8*(6), pp.24-31.

Tak, B.C., Urgaonkar, B. and Sivasubramaniam, A., 2011. To Move or Not to Move: The Economics of Cloud Computing. In *HotCloud*.

Talia, D., 2011, July. Cloud Computing and Software Agents: Towards Cloud Intelligent Services. In *WOA* (Vol. 11, pp. 2-6).

Tao, J. Marten, H. Kramer, D. and Karl W., 2011. An Intuitive Framework for Accessing Computing Clouds, Procedia Computer Science, vol. 4, no. 1, pp. 2049–2057, Jan. 2011.

Taylor, R.C., 2010. An overview of the Hadoop/MapReduce/HBase framework and its current applications in bioinformatics. BMC bioinformatics, 11(12), p. S1. Vancouver

Tekinerdogan, B., Özturk, K. and Dogru, A., 2011, June. Modeling and reasoning about design alternatives of software as a service architectures. In *Software Architecture (WICSA), 2011 9th Working IEEE/IFIP Conference on*(pp. 312-319). IEEE.

Tippit Inc., 2008. Web Hosting Unleashed: Cloud-computing services comparison guide. Available from: http://www.itsj.com/Resources/cloudcomputing-comparison.pdf [Accessed 7 January 2016]

Tolk, A., 2013. Interoperability, Composability, and their Implications for Distributed Simulation. In: *17th IEEE/ACM International Symposium and Real Time Applications*, pp.3-9. IEEE Press (2013).

Toosi, A. N., Calheiros, R. N. and Buyya, R., 2013. Interconnected Cloud Computing Environments: Challenges, Taxonomy and Survey, *ACM Computing Survey*, Vol. 5, Article A.

Topology and Orchestration Specification for Cloud Applications (TOSCA). Version 1.0. OASIS Standard (2013).

Toivonen, M., 2013. Cloud Provider Interoperability and Customer Lock-in. Dept. of Computer Science, University of Helsinki, Research Paper.

Tran, V., Keung, J., Liu, A. and Fekete, A., 2011, May. Application migration to cloud: a taxonomy of critical factors. In *Proceedings of the 2nd international workshop on software engineering for cloud computing* (pp. 22-28). ACM.

Silas, S., Rajsingh, E.B. and Ezra, K., 2012. Efficient service selection middleware using ELECTRE methodology for cloud environments. *Information Technology Journal*, *11*(7), p.868.

Ubuntu Juju, 2015. Available from: https://juju.ubuntu.com [Accessed 17 September 2016]

Vanberg, A.D. and Ünver, M.B., 2017. The right to data portability in the GDPR and EU competition law: odd couple or dynamic duo? *European Journal of Law and Technology*, *8*(1).

Varia, J., 2008. 'Cloud Architectures'. Whitepaper, [online].

Varia, J., 2010. 'Architecting for the Cloud: Best Practices'. Whitepaper [online].

Vu, Q.H. and Asal, R., 2012. Legacy application migration to the cloud: Practicability and methodology. In *Services (SERVICES), 2012 IEEE Eighth World Congress on* (pp. 270-277) June. IEEE.

Walsham, G., 1995. Interpretive case studies in IS research: nature and method. European Journal of Information Systems. [Online]. 4 (2). p.pp. 74–81. Available from: http://www.palgrave-journals.com/doifinder/10.1057/ejis.1995.9.

Wang, L., Von Laszewski, G., Younge, A., He, X., Kunze, M., Tao, J. and Fu, C., 2010. Cloud computing: a perspective study. In *New Generation Computing*, *28*(2), pp.137-146.

Wang, R., 2013. Adopting Cloud Computing: Seeing the Forest for the Trees [online]. Available from: http://www.forbes.com/sites/oracle/2013/09/20/adopting-cloudcomputing-seeing-the-forest-for-the-trees/ [Accessed on 12th February 2014].

Wang, R. R., 2012. The Enterprise Cloud Buyer's Bill of Rights: SaaS Applications. *How to maximize your investment and avoid potential Vendor lock-in*, Best Practices Report.

Ward, C., Aravamudan, N., Bhattacharya, K., Cheng, K., Filepp, R., Kearney, R., Peterson, B., Shwartz, L. and Young, C.C., 2010. Workload migration into clouds challenges, experiences, opportunities. In *Cloud Computing (CLOUD), 2010 IEEE 3rd International Conference on* (pp. 164-171) July. IEEE.

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

Weerawarana, S., Curbera F., Leyman, F., Storey, T. and Ferguson, D.F., 2005. Web Services Platform Architecture. [online].

Weinhardt C, Anandasivam A, Blau B, Borissov N, Meinl T, Michalk W, Stößer J., 2009. Cloud computing–a classification, business models, and research directions. Business & Information Systems Engineering. Oct 1;1(5):391-9.

Wettinger, J., Behrendt, M., Binz, T., Breitenbücher, U., Breiter, G., Leymann, F., Moser, S., Schwertle, I., Spatzier, T., 2013. Integrating Configuration Management with Model-driven Cloud Management based on TOSCA. In: 3rd International Conference on Cloud Computing and Service Science (CLOSER), pp. 437–446. SciTePress, Aachen

Wettinger J, Breitenbücher U, Leymann F., 2014. DevOp Slang—bridging the gap between development and operations. In: Villari M, Zimmermann W, Lau KK (eds) Service-Oriented and Cloud Computing. Lecture Notes in Computer Science, vol. 8745. Springer, Berlin Heidelberg, pp 108–122

Wettinger J, Gorlach K, Leymann F., 2014. Deployment aggregates—a generic deployment automation approach for applications operated in the cloud. In: IEEE 18th International Enterprise Distributed Object Computing Conference Workshops and Demonstrations (EDOCW), pp 173–180

Wettinger, J., Breitenbücher, U., Leymann, F., 2014. Standards-based Devops automation and integration using tosca. In: Proceedings of the 7th International Conference on Utility and Cloud Computing (UCC 2014), pp. 59–68. IEEE Computer Society

Wettinger, J. Andrikopoulos, V. Strauch, S. and F. Leymann., 2013. Enabling Dynamic Deployment of Cloud Applications Using a Modular and Extensible PaaS Environment, in Proceedings of IEEE CLOUD. IEEE Computer Society, pp. 478–485.

World Economic Forum (WEF), 2011. Advancing Cloud Computing: What to do now? *Priorities for Industry and Governments*, WEF in Partnership with Accenture.

Web Service Description Language (WSDL) 2016, [online]. Available from: http://www.w3.org/tr/wsdl/ [Accessed on 24 December 2016].

Yang, H. and Tate, M., 2012. A descriptive literature review and classification of cloud computing research. *Communications of the Association for Information Systems*, *31*(2), pp.35-60.

Yoo, X. S., 2010. Cloud Computing: Architectural and Policy Implications, [online]. Available from: http://techpolicyinstitute.org/files/yoo%20architectural_and_policy_implications.pdf [Accessed 27 April 2014].

Youseff, L., Butrico, M. and Da Silva, D., 2008. Toward a unified ontology of cloud computing. In *2008 Grid Computing Environments Workshop* (pp. 1-10) November. IEEE.

Yu, D., Wang, J., Hu, B., Liu, J., Zhang, X., He, K. and Zhang, L.J., 2011, July. A practical architecture of cloudification of legacy applications. In *Services (services), 2011 IEEE world congress on* (pp. 17-24). IEEE.

Zardari, S. and Bahsoon, R., 2011, May. Cloud adoption: a goal-oriented requirements engineering approach. In *Proceedings of the 2nd International Workshop on Software Engineering for Cloud Computing* (pp. 29-35). ACM.

Zenga, S. X., Xie, X. M., & Tam, C. M., 2010. Relationship between cooperation networks and innovation performance of SMEs. Technovation, 30(3), 181–194.

Zhao, J.F. and Zhou, J.T., 2014. Strategies and methods for cloud migration. *international Journal of Automation and Computing*, *11*(2), pp.143-152.

Zhang, Q., Cheng L., & Boutaba, R., 2010. Cloud computing: state-of-the-art and research challenges. Journal of Internet Service Application 1(1):7–18. doi:10.1007/s13174-010-0007-6

Zhang, Z., Wu, C. and Cheung, D.W., 2013. A survey on cloud interoperability: taxonomies, standards, and practice. *ACM SIGMETRICS Performance Evaluation Review*, *40*(4), pp.13-22.

Zhu K. X. and Zhou, Z. Z., 2011. 'Lock-in Strategy in Software Competition: Open-Source Software vs. Proprietary Software'. Information Systems Research.

Zikmund WG., 2000. Business Research Methods, 6th edn. the Dryden Press, Chicago, IL

List of Abbreviations

AHP	Analytic Hierarchy Process
AMD	Advanced Micro Devices
ANOVA	Analysis of Variance
API	Application Programming Interface
ARAPNET	Advanced Research Projects Agency Networks
ARM	Advanced RISC Machines
ASP	Application Service Provider
AUP	Acceptable Use Policy
AWS	Amazon Web Services
BCS	British Computer Society
BPaaS	Business Process as a Service
BPEL	Business Process Execution Language
BPM	Business Process Management
BPMN	Business Process Modelling Notation
CAMP	Cloud Application Management Platforms
CCaaS	Compute Capacity as a Service
CCMP	Common Cloud Management Platform
CCRA	Cloud Computing Reference Architecture
CDMI	Cloud Data Management Interface
CDMI	Cloud Data Management Interface
CEO	Chief Executive Officer
CIMI	Cloud Infrastructure Management Interface

CIO	Chief Information Officer
CISC	Complex Instruction Set Architectures
COBIT	Control Objectiveness for Information and Related Technologies
CPU	Central Processing Unit
CRM	Customer Relationship Management
CSA	Cloud Security Alliance
CSC	Cloud Service Customers
CSP	Cloud Service Provider
CTO	Chief Technology Officer
DAR	Data at Rest
DCN	Data Centre Network
DDoS	Distributed Denial of Service
DevOps	A clipped compound of “Development” and “Operations”
DIT	Data in Transit
DIU	Data in Use
DMTF	Distributed Management Task Force
DPA	Data Protection Act
DSL	Domain Specific Language
EA	Enterprise Architecture
EC	European Commission
EC2	Elastic Compute Cloud
EEA	European Economic Area
EII	Enterprise Information Integration
ENISA	European Network and Information Security Agency

ERP	Enterprise Resource Planning
ETSI	European Telecommunications Standard Institute Technical Community
GAE	Google App Engine
GQL	Google Query Language
HIPAA	Health Insurance Portability and Accountability Act
HTTP	Hypertext Transfer Protocol (HTTP)
I/O	Input/output
IaaS	Infrastructure-as-a-Service
ICO	Information Commissioner's Office
ICT	Information and Communication Technology
IDC	International Data Corporation
IEC	International Electro-technical Commission
IEM	Identity, Entitlement, and Access Management
IP	Internet Protocol
IS	Information Systems
ISACA	Information Systems Audit and Control Association
ISO	International Standards Organisation
ISV	Independent Service Vendors
ITIL	Information Technology Infrastructure Library
ITU-T	International Telecommunication Unit
J2EE	Java Platform Enterprise Edition
JISC	Joint Information Systems Committee
JSON	JavaScript Object Notation
KVM	Kernel-based Virtual Machine

LOB	Line of Business
MAS	Multi-Agent Systems
MCDM	Multi-Criteria Decision-Making
MDA	Model Driven Architecture
MDE	Model Driven Engineering
MySQL	Open Source Relational Database Management System (RDBMS)
NAS	Network Attached Storage
NIST	National Institute of Standards and Technology
NoSQL	Non-SQL, Non-relational or Not only SQL
OCCI	Open Cloud Computing Interface
OCCI	Open Cloud Computing Interface
OCCI	Open Cloud Computing Interface
OGF	Open Grid Forum
OMG	Object Management Group
OMG	Object Management Group
ORDBMS	Object-Relational Database Management Systems
OS	Operating System
OVF	Open Virtualization Format
OWL	Web Ontology Language
P2V	Physical-to-Virtual
PaaS	Platform-as-a-Service
PC	Personal Computer
PCI-DSS	Payment Card Industry – Data Security Standard
PDP	Platform Deployment Package

PGR	Post Graduate Researcher
PHP	recursive acronym for Hypertext Pre-processor
QoS	Quality of Service
QSR	Qualitative Research Software
RBAC	Role-Based Access Control
RDF	Resource Description Framework
REST	Representational State Transfer
RFI	Request for Information
ROI	Return on Investment
S3	Simple Storage Service
SaaS	Software-as-a-Service
SAML	Security Assertion Mark-up Language
SAN	Storage Area Network
SAN	Storage Area Network
SAP	Systems, Applications and Products in data processing
SCM	Supply Chain Management
SDDC	Software Defined Data Centre
SJAX	Synchronous JavaScript and XML
SLA	Service Level Agreement
SLR	Systematic Literature Review
SMEs	Small to Medium-sized Enterprises
SNIA	Storage Networking Industry Association
SOA	Service Oriented Architecture
SOAP	Simple Object Access Protocol

SPARQL	recursive acronym for SPARQL Protocol a d RDF Query Language
SQL	Structured Query Language
SQL	Structured Query Language
SSL	Secure Socket Layer
STaaS	Storage as a Service
SWRL	Semantic Web Rule
TCO	Total Cost of Ownership
TCP	Transmission Control Protocol
TFEU	Treaty on the Functioning of the European Union
TLS	Transport Layer Security
TOSCA	Topology and Orchestration Specification for Cloud Applications
UDDI	Universal Description, Discovery and Integration
UI	User Interface
VHD	Virtual Hard Disk
VM	Virtual Machine
WAN	Wide Area Network
WEF	World Economic Forum
WORA	Write Once Run Anywhere
WSDL	Web Service Description Language
X86	Backward-Compatible Instruction Set Architectures

APPENDIX 1

Systematic Review Protocol

APPENDIX 1

Cloud computing is a technology that is already a part of many IT environments. The growing popularity of cloud computing services have encouraged many IT organisations to switch from privately owned data centres to third party managed clouds. However, the diversity and heterogeneity of today's existing cloud offerings raises several interoperability and portability challenges which introduces migration barriers due to the vendor lock-in problem. From an enterprise perspective, the vendor lock-in problem is widely recognised as a major inhibitor to cloud adoption. Unfortunately, research on factors intensifying and/or triggering a lock-in situation in the cloud, as well as research investigating the socio-technical, business and legal issues related to cloud lock-in is limited. To date, few studies have addressed the lock-in problem within the context of a systematic literature review. The main objective of this appendix (1) is to obtain a holistic view of cloud SaaS migration approaches, benefits and limitations in existing cloud migration research field. The identification of primary studies in this systematic review is based on a predefined research protocol with a research question, inclusion and exclusion criteria, and a search strategy. The analysis of included studies indicates that there are several challenges of vendor lock-in affecting enterprise migration to cloud-based systems. Author summarised the associated lock-in challenges into three main categories, namely: 1) Technical or technological barriers 2) Business environment issues, and 3) Legal and political risks. The classification of challenges identified not only illustrate the complexity of the vendor lock-in problem in the cloud environment, where IT practitioners are aggressively moving applications and data to, but also show the limitations that companies (and cloud customers) face when selecting/sourcing and implementing vendor-neutral interoperable and portable cloud services. Moreover, these challenges also represent current research gaps and opportunities for future research direction. As an example, this analysis has also confirmed that there is a need to provide a cloud decision framework to assist enterprise decision-makers and IT practitioners to avoid the risks of vendor lock-in when implementing or migrating between cloud-based solutions and vendors within existing environment – thereby, reinforcing on the need to fulfil objective 6 (i.e. O.6) of this PhD thesis.

1.0 Background

According to the Cisco Global Cloud Index 2014 report (Pardo et al. 2016), cloud usage is growing by 300% by the end of 2018, while traditional data centres are dwindling down to a global decline. The cloud computing industry will continue to see healthy expansion as strong data reflects an increase in sales, adoption and business acceptance. Forecasts for global cloud adoption are bullish. For example, Forrester believes that businesses will spend about $191 billion on cloud services by 2020, compared to $72 billion in 2014 (King, 2014). This projection suggests that the future cloud market will be 20 percent larger than what had previously been forecasted by the firm, which reveals that the sector has entered a "hypergrowth" stage and is displacing on-premise setups faster than expected. Further, International Data Corporation (IDC) predicts the cloud computing market in 2017 will be worth $107 billion, over twice as much as its 2013 estimate of $47.4 billion (Casemore, 2014). In this aspect, a key trend shaping the cloud ecosystem over the next several years is the continued prominence and even quicker rise of Software-as-a-Service (SaaS), widely expected to show the strongest growth in both revenues and deployments. One prediction in this respect is that in 2016, worldwide SaaS revenues will total approximately $106 billion (Cisco, 2015). Other forecasts call on more than $132 billion in sales of SaaS by 2020, or a $50.8 billion revenue in 2018 from SaaS-based business applications alone (Columbus, 2014). Furthermore, on the report of Gartner (2016), by 2020, a corporate "no-cloud" policy will be as rare as a "no Internet" policy is today. Therefore, while research confirms the widespread adoption and usage of cloud computing services across enterprises, arguably it could be said primarily of cloud computing as a business phenomenon rather than a technological one.

Currently, cloud computing services are finding more applications in business, and extensive attention in the industry. The United Kingdom (UK) is an important market for United States (US) cloud vendors because of its developed economy, established base of business customers who understand the cloud value proposition and the lack of infrastructural hurdles present in other countries. Previously, the UK cloud computing market was estimated to reach around £10.5 Billion, up from £6.1Billion in 2010 [2]. More recently, according to IDC (2010) report, the UK IT market is valued at around £20Bn with cloud associated revenues growing to around 20% of that by 2015. Moreover, recent research from Cloud Industry Forum (2015) suggests that by the end of 2015, over 90% of UK organisations (up from 78% in 2014) will have formally adopted at least one cloud service. In addition, according to the research reported in (Opara-Martins et al. 2015), over 50% of UK businesses are already using cloud services, while a greater majority (69%) utilise a combination of cloud services and internally owned applications (hybrid IT) for organisation needs. However, concerns about data protection and security, as well as regulatory compliance make UK clients wary of handing over control of their data. On a global scale, due to concerns about the viability of transatlantic data transfers in the face of the new Brexit Bill, some U.S. companies, for instance, have built or are considering establishing data centres in the United Kingdom and other European countries.

Despite the increasing usage of cloud computing services, there are also some challenges associated with the adoption of cloud computing in the enterprise. Example of such challenges holding back adoption and migration to cloud computing include vendor reliability questions, fears of vendor lock-in and reluctance to depend on an Internet connection for access to a company's data (Martson et al. 2011; Pardo et al. 2016). There is also a general preference for such data to be physically stored in the UK or at least in Europe, especially among public sector and smaller clients within the UK and EU region (Opara-Martins et al. 2015). Given these challenges, it is understandable that data lock-in and data transfer issues are the two major obstacles of cloud computing (Armbrust et al. 2009) presently, and are currently on the European union's list of research topics (Schubert et al. 2010, p.3). For instance, application and data migration to and within the cloud environment is still a mostly unsolved research problem (Khajeh-Hosseini et al. 2010), due to the risks of vendor lock-in (Catteddu and Hogben, 2009). Vendor lock-in frees cloud computing vendors to establish non-competitive prices, since they have become in effect "sole source" of a given cloud-based technology product or service. Therefore, in Appendix 1, author investigates the vendor lock-in problem within credible cloud migration literature sources to identify, analyse and classify existing risks to cloud SaaS lock-in, and highlight unsolved and unresolved challenges in the road to successful migration.

As deliberated thus far within this thesis, vendor lock-in problem within the cloud environment often rests on proprietary data structures (i.e. formats) and supposed intellectual property (IP) rights which may also result from standards controlled by the vendor. Thus, in a vendor lock-in situation, applications and data cannot be transferred to a different cloud provider without incurring significant switching costs (Opara-Martins et al. 2016). Such a situation is triggered or intensified by the differences that exist between various cloud service offerings from different providers. This difference is caused by the heterogeneity of cloud semantics, technology and interfaces that limits application and data portability and interoperability. Cloud semantics refers to the description of a cloud service by its provider (Nelson and Uma, 2012). Cloud technologies comprise the middleware and applications used to support a cloud service. Cloud interfaces are the common Application Program Interfaces (APIs) that provide programmatic access to the services offered by a cloud vendor. These APIs expose the semantics and technologies used by a provider, and play a key role in providing access to the service management functionality. As a result, their heterogeneity across different clouds is deemed a major barrier to cloud portability and interoperability (Rodero-Merino et al. 2010; Sampaio and Mendonça, 2011; Tao et al. 2011). Hence, cloud users are often locked-in to a specific cloud provider due to the significant differences in the semantics (Emmerich and Galán, 2009), technologies (Rochwerger et al. 2009), and interfaces (Rodero-Merino et al. 2010) adopted by different providers. These differences hinder cloud portability and interoperability (Hofmann and Woods, 2010). Therefore, data and applications deployed on a cloud can become locked in to the cloud provider, due to the way in which the application uses the semantics, technologies and APIs of the provider (Abu-Libdeh et al. 2010). Admittedly, some of the downside of vendor lock-in can be off-set by savings resulting from 1) shorter learning curves, 2) development (i.e. porting) costs absorbed by the vendor due to incompatibility issues caused because of controlling a large (user) business base, and 3) investment costs for commercial cloud-based technologies and derivative software product offerings that can benefit enterprise software systems (Wydler, 2014).

Viewing the cloud computing lock-in problem from a technical perspective may be too narrow to comprehensively analyse such a complex situation. Instead, complexity of cloud lock-in situations can originate from many other sources than the service (i.e. cloud or on-premise IT) system itself (Benedettini and Neely 2012). In information system (IS) research, for example, such IT systems are considered as socio-technical systems involving technological components as well as people and the organizational environment interacting with it (Picot and Baumann 2009; Orlikowski 1992; Belfo 2012). In the same vain, author follows this research discipline to see cloud computing as a concept involving engineering as well as various management aspects. Thus, it needs a socio-technical approach to assess its characteristics and related lock-in risks from a holistic view. To this end, the main objective of this systematic review study is to obtain a holistic understanding of the vendor lock-in risks associated with cloud migration research and investigate the influence such risk(s) have on enterprise decisions to adopt cloud-based SaaS solutions. Hence, the study presented here provides a concise yet relevant discussion and analysis of the current state of cloud computing migration and associated SaaS lock-in challenges with some fundamental guidelines that should be observed by organisations entering a cloud computing service contract. In contrast to existing works, this part of the PhD study extends the scope of cloud computing migration beyond one specific challenge area, instead it addresses the vendor lock-in problem from three main perspectives or categories (i.e. technical, business, and legal) – thereby contributing substantially to the growing body of knowledge on cloud computing. Therefore, author summarises the contributions made by this review study as follows:

- To help researchers (i.e. academia) and practitioners (i.e. industry) in the cloud computing community have a deep understanding of the current state of cloud computing (SaaS) migration approaches proposed in literature, associated vendor lock-in challenges and limitations, as well as understand insightful findings and recommendations to be learned.
- To provide a comprehensive view of cloud SaaS migration challenges, specifically concerned with decision frameworks, tools, and processes for cloud-to-cloud migration and legacy-to-cloud migration (or vice-versa), that need to be investigated further – hence a prelude to further research activities can be opened.

The rest of the appendix 1 is structured as follows. Section 2 discusses related work. Section 3 presents the systematic literature methodology applied in this review study. Section 4 outlines the key findings. This section

also provides discussion and implication of this systematic review findings, followed by conclusion and directions for future work in Section 5.

2.0 Related Work

Several related works and publications exist in the literature, emphasizing the importance and need to avoid vendor lock-in risks when migrating enterprise systems\data to and within the cloud computing environment. However, author did not identify any study with a sole focus on cloud SaaS migration to address directly the related elements which intensifies and/or triggers a cloud lock-in situation. Researchers only identified some generic studies that were conducted to discuss specific interoperability and portability aspects of the cloud lock-in problem. Therefore, the related work presented herein discuss approaches and models to build interoperable and portable frameworks to support cloud migration, and informed decisions to avoid vendor lock-in risks in the enterprise. Note, these studies have been selected because they share similar concerns as per the review questions (*see **Section 3.1***).

Previous studies, hitherto, provide a partial understanding of certain aspects of cloud migration in general, they do not provide a comprehensive framework of how the SaaS migration decisions is to be carried out and organised from a decision framework perspective to avoid vendor lock-in risks in cloud computing environments. The review of existing literature reveals that a systematic review protocol for characterising the associated risks of vendor lock-in, affecting enterprise migration to cloud computing SaaS environments is yet to be provided. Moreover, it is suggested also that the lack of review articles has been hindering the progress of information systems (IS) field (Webster and Watson, 2002). This calls for a need to contribute a review study that distils cloud SaaS migration approaches to understand the associated migration challenges, and what essential activities, tasks, and decisions are involved during the cloud-to-cloud migration or legacy-to-cloud SaaS modernisation/replacement. Thus, in this section we considered it useful to conduct a systematic review with the primary objectives: to firstly, summarise the empirical evidence of the approaches, benefits and limitations in the existing cloud migration research; secondly, to identify any gaps in current research tackling the vendor lock-in problem and cloud SaaS migration specifically, in order to suggest areas for further investigation and; thirdly, to provide a decision framework with guidelines as a prelude to further research activities to tackle the vendor lock-in risks in cloud computing environment. However, considering most research in cloud computing migration (in industry and academia) generally starts with a literature review of some sort. The literature review is an essential approach to conceptualise research areas and synthesise prior research which directly contributes to a cumulative research culture (Webster and Watson, 2002). Therefore, unless the literature review is thorough and fair, it is of little scientific value (Keele, 2007); thus, our main rationale for undertaking a systematic review in this study.

3.0 Research Methodology

A literature review can be conducted in four different methods, namely: Narrative Review, Descriptive Review, Vote Counting, and Meta-Analysis. These four review methods are placed in a qualitative-quantitative continuum to illustrate their different focuses (King and He, 2005). In this paper, we found descriptive review as the most appropriate approach for the current phase of our research study. A descriptive review focuses on revealing an interpretable pattern from the existing literature (Guzzo et al., 1987). It produces some quantification, often in the form of frequency analysis, such as publication time, research methodology, and research outcomes. Such a review method often has a systematic procedure including searching, filtering, and classifying processes. First a reviewer needs to conduct a comprehensive literature search to collect as many relevant papers as possible in an investigated area. Then the reviewer treats an individual study as one data record and identifies trends and patterns among the papers surveyed (King and He, 2005). The outcome of such a review is often claimed to be representative of the current state of a research domain. Accordingly, by comprehensively reviewing existing studies on cloud migration approaches and associated lock-in challenges, we thus position this review study as the newest reference point for cloud computing research and practice.

Therefore, the adopted methodology allowed us to classify/categorise, from different perspectives (e.g. technical, business etc.), the main vendor lock-in risk factors for cloud SaaS migration, and taking into

consideration crucial security and legal challenges (e.g. data ownership, portability, exit strategy etc.). This methodological approach resulted on a comprehensive analysis of selected cloud migration research studies provided as basis for analysis, hence promoting the need of a decision framework to avoid vendor lock-in risks for adoption and migration to cloud computing.

3.1 Review Questions

More specifically, this review aims to answer the following questions (review question is abbreviated as RQ):

RQ.I. What are the associated risks factors of vendor lock-in affecting enterprise migration to cloud computing SaaS environments?

RQ.II. What are the existing tasks, methods, techniques, activities and decisions available to support avoiding vendor lock-in when migrating or switching between SaaS vendors/services and on-premise systems?

RQ.III. How is cloud migration reported within existing research theme?

- What are the fora or communities in which work on cloud migration has been published?
- What evaluating procedures have been used to assess the results in each paper? What is maturity level of the research in the cloud SaaS migration field?

RQ.IV. What are the emerging standards available to mitigate vendor lock-in risks and achieve portability and interoperability of cloud services? In addition, what are the potential of developer and operations (shortened to DevOps) tools such as Chef, Puppet and Juju to tackle the cloud vendor lock-in problem?

RQ.V. What are the strategies to avoid and mitigate vendor lock-in risks when migrating computing resources from on-premise to the cloud environment?

3.2 Developing the Review Protocol

Note, these questions have been specifically formulated to aid authors in defining and evaluating the review protocol to be used in this study. Considering the review questions drive the entire systematic review methodology, the questions listed above have been structured based on the PICOC (Population, Intervention, Comparison, Outcome and Context) criteria suggested by (Petticrew and Roberts, 2005) to frame research questions. A question on population may refer to a very specific cloud service customer group with different experience level. The population might be any of the following: specific role, application area and industry group. Intervention is the systematic methodology, tool, framework or procedure (with guidelines) that addresses a specific issue. Comparison is the procedure or migration approach with which the intervention is being compared. Outcomes relate to factors of importance to the cloud service consumers and practitioners. As per the last criteria, it refers to the context in which the comparison takes place (e.g. academia or industry), the participants taking part in the study, and the tasks being performed. Using the recommended PICOC criteria, we define our review question elements as:

- **Population**: enterprise stakeholders/decision makers, consumers, project managers or developers within the cloud computing and/or SaaS IT application domain
- **Intervention**: cloud migration, SaaS lock-in, vendor lock-in, cloud lock-in
- **Comparison**: cloud-to-cloud migration, inter-cloud migration, legacy on-premise application, software application rationalisation/modernisation
- **Outcome**: systematic decision framework and guidelines with prescriptive and emergent strategies to mitigate SaaS lock-in risks for enterprise cloud adoption and migration
- **Context**: the context in which the comparison takes place is academia and industry. Note, this is because many cloud migration research and experimental studies that take place in academia use student participants and small scale tasks. Such studies, however, are unlikely to be representative of what might occur with practitioners working in industry – hence our context incorporates both.

The procedure for conducting this descriptive review process is described in the next section.

3.3 Planning the Review

Existing guidelines for systematic reviews have slightly different proposals about the number and order of activities, however in **Figure 1** we designed a systematic review protocol for use in this study. The review protocol was prepared by the first author and reviewed by the other two authors. As depicted, **Figure 1** divides the stages of our review protocol into three main phases, namely: Planning the review, Conducting the review and Reporting the review. We now summarise all phases of our research methodology concisely and precisely, below.

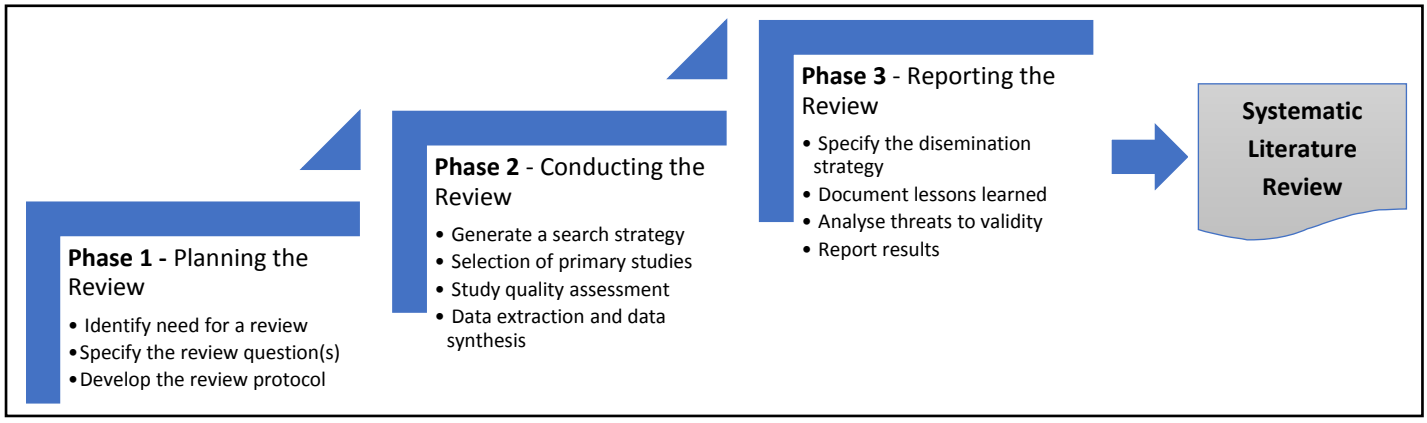


Figure 1. Overview of Our Research Process

3.4 Establishing the Need for a Systematic Review

The need for a systematic review arises from the requirement of authors to summarise existing information about the vendor lock-in phenomenon affecting enterprise migration to cloud computing SaaS environments, in a thorough and unbiased manner. This need has already been identified and the contributions of this systematic review justified in the paragraphs above, in addition to the review questions and their objectives which have been specified accordingly in paragraph(s) 1, 2, and 3 of Appendix 1. The questions, however, are based on the initial enterprise motivation scenario (discussed earlier in **Section 2**). The protocol, being a critical element of any systematic review, have been reviewed and evaluated by authors PhD research supervisors. List of RQ identified above have been adapted to assist the evaluation of this systematic review protocol. Developing the evaluation process for the review protocol includes several stages such as search strategy, selection criteria, quality assessment criteria, data extraction and synthesis strategy (Rai et al. 2015). These stages are further explored in the next phase of our systematic review process.

3.5 Conducting the Review with a Defined Search Strategy

In this review study, attempts have been made to examine all the papers that have been published on cloud computing and SaaS lock-in challenges, and includes novel methods or interesting idea in this aspect. Hence, the review aims at collecting and investigating all the credible and effective studies that have examined cloud computing migration challenges. However, focusing on limited outlets cannot be justified for a literature review on vendor lock-in risks in cloud computing migration, as the publication channels are still scattered. In the meantime, using online database searches as a primary literature collecting approach has become an emerging culture among IS researchers who are interested in contemporary phenomena (Hwang and Thorn, 1999; Hwang and Li, 2010; Petter and McLean, 2009; Sabherwal, Jeyaraj, and Chowa, 2006). Therefore, for a literature review on cloud computing, it is appropriate and practical to focus on online databases rather than library collections (Yang and Tate, 2012).

The search strategy used in our review study was developed in accordance to the guidelines of (Keele, 2007) and in consultation with librarians at authors university. This search strategy was mainly guided by the review questions (in **Appendix 1**) by breaking down the question(s) into individual facets i.e. population, intervention, comparison, outcomes and context, as identified in the PICOC criteria above. This is then followed by drawing

up a list of synonyms, abbreviations, and alternative spellings (i.e. keywords) which are linked together by using the Boolean ORs and ANDs. Using the appropriate Boolean expressions, a set of sophisticated search strings were generated as shown in **Table 1**. The keywords and sophisticated search strings constructed in **Table 1** are derived from the review questions and defined by using PICOC method. Distinct search strings from **Table 1** were applied to the following electronic digital databases of relevance to our research field, some of these includes: Springer Link, IEEE Xplore, ACM Digital Library, Google Scholar, Citeseer Library, Mendeley, Inspec by IET, ScienceDirect, Wiley Online Library, Organisation reports and white papers published by standards initiative groups and companies working on cloud computing (e.g. CSA, OpenGroup, NIST, ENISA, ETSI, ITIL, Gartner, OpenStack, IBM etc.). This resulted in an extraction of numerous peer reviewed literature from years 2010 to 2017 (i.e. 7 years' period).

Table 1. Composition of Sophisticated Search Strings

RQ. No	Keywords	Search Strings
RQ.I	Risks, challenges, obstacles, issues, concerns, problems, constraints, cloud SaaS applications, migration, vendor lock-in, inter-cloud lock-in	(Challenges OR Issues OR Problems OR Vendor lock-in OR Risks OR Provider lock-in OR Constraints OR Inter-lock-in) AND (Cloud computing OR Enterprise Migration OR Cloud Migration OR SaaS environment OR BYOD OR SaaS Migration)
RQ.II	Frameworks, tools, decisions, decision-making, standards, tasks, methods and techniques, cloud migration	(Cloud computing OR Cloud migration OR SaaS migration OR Switching OR Evolution OR Cloudification OR Adaptation OR Rationalisation OR Modernisation OR Reengineering OR Integration OR Monolithic OR Micro-services) AND (Tools OR Frameworks OR Methodology OR Decision-making OR Decision support OR Standards OR Process OR Benchmark OR Cloud application)
RQ.III	Cloud migration, current state, existing research, research contribution, cloud maturity, SaaS maturity	(Cloud computing OR SaaS migration OR SaaS application OR Adoption OR Evolution OR Cloud software) AND (Current state OR Cloud maturity OR SaaS maturity)
RQ.IV	Standards, regulatory bodies, compliance, interoperability, portability, cloud services, cloud migration, enterprise adoption and migration, proprietary lock-in, vendor lock-in, cloud computing	(Cloud computing OR Standards OR Opensource cloud OR Portability OR Interoperability OR Lock-in OR Cloud migration OR Cloud APIs) AND (Cloud lock-in OR SaaS Lock-in OR DevOps tools OR Cloud migration OR Enterprise migration)
RQ.V	Strategies, guidelines, best practice, risk mitigation cloud migration, legacy system, ICT, on-premise system, vendor lock-in, cloud computing	(Strategies OR Guidelines OR Best practices OR Reference model OR Framework OR Methodology OR Cloud computing OR SaaS Cloud application) AND (Cloud migration OR Migration to cloud OR Legacy to cloud migration OR Cloud to cloud migration OR Intercloud migration) AND (Vendor lock-in OR SaaS lock-in OR Vendor neutral OR Provider Lock-in OR Lock-in avoidance OR Cloud infrastructure OR Cloud Architecture)

Once the potentially relevant primary studies were obtained, they were further assessed for their actual relevance based on the following inclusion and exclusion criteria (in **Table 2**) for quality assessment. Each article was examined in its entirety, including abstract, text, and tables to provide direct evidence about the RQ before selection. In addition to the articles themselves, any published follow-up articles or comments by either the author(s) or another researcher were examined for information relating to cloud migration and SaaS lock-in risks. In each study, if it was required to be familiar with some concepts and methods and to read further on the topic, other books and papers are proposed and referred to. The result of this effort is a comprehensive collection of resources that can provide an acceptable level of concepts and information about the vendor lock-in problem in migration to cloud computing environments and the different views of addressing this problem that are introduced in the literature.

Reference snowballing was also conducted manually to identify additional relevant articles through the list of references found using search strings. Accordingly, research studies that did not meet the inclusion criteria mentioned in **Table 2** were excluded. Thus, 64 studies in total were included in our systematic review. Amongst the included studies, each journal and conference proceedings was reviewed by the first author and the papers that addressed RQ of any type were identified as potentially relevant. The researcher responsible for searching

the specific journal or conference applied the detailed inclusion and exclusion criteria to the relevant papers. Note, we included articles in our study where the literature review was only one element of the articles contribution as per addressing any of the initial RQ, as well as studies for which the literature review was the main purpose of the paper. Data extracted from each study were: The author(s) and the journal or conference full reference, Year of publication (addressing RQ.III), Migration type (addressing RQ.II and RQ.III), Unit of migration (addressing RQ.II and RQ.III), Cloud deployment model (addressing RQ.I and RQ.II), Study contribution type (addressing RQ.III), Publication channel (addressing RQ.III), and citation impact. For analysis purpose, the data extracted from each study was tabulated to show: the number of cloud migration research published per year and their distribution by publication channel (addressing the first part of RQ.III); the number of studies in each major (or active) research fora or communities (addressing the second part of RQ.III) and; the distribution of studies per their contribution type and evaluation method (addressing the third part of RQ.III). However, the next stage will be to record the extracted data from the selected studies and perform data synthesis of included primary studies per the recommended guidelines of (Kitchenham, 2004). The objective of the data synthesis is to collate and summarise the results of the included primary studies.

Table 2. Inclusion and Exclusion Criteria

	CRITERIA
INCLUSION	▪ Decision making frameworks and systems aiding cloud service customers rank, evaluate and select the cloud providers that fit legacy and SaaS application requirements
	▪ Papers based on composed search strings and which content matches the research questions
	▪ Studies that primarily focuses on answering the review questions and contains cloud migration and SaaS lock-in aspects
	▪ Studies in the form of scientific peer-reviewed paper
	▪ Studies that propose solution, experience, or evaluation of cloud migration
EXCLUSION	o Editorials and Abstract
	o Papers not subject to peer review
	o Studies in language other than English were generally excluded from the review
	o Duplicate reports of the same study (note, when several reports of a study exist in different journals the most complete version of the study was included in the review)

3.6 Reporting the Review

The final phase of our systematic review study involves writing up the results of the review and communicating the results effectively to potentially interested parties. Herein, we present the results based on the review questions that were defined in **Appendix 1** and as per the review protocol presented in **Figure 1** respectively. The RQ.I has already been answered (in **Section D**) and the associated risk factors (or elements) of vendor lock-in affecting enterprise migration to cloud computing SaaS environment have been identified, including the classification of tasks, activities, and decision steps to avoid vendor lock-in risks when migrating or switching between cloud SaaS vendors (and on-premise systems). Note, that the migration decision steps, tasks, and supporting activities discussed (as per RQ.II) have been identified from selected secondary sources (see reference list) and the primary studies cited in **Table 3**. To examine the state of research on cloud computing SaaS migration we broadly answer RQ.III under the result and discussion section below. We considered the research community or fora with the highest publication count in our review (Table 6), the individual researcher(s), the organisations/institutions to which researchers are affiliated with (Table 7) and the country in which the authors' is situated (Table 8). The other part of this question regarding maturity level in the cloud SaaS field is also illustrated in **Section D** using Figure(s) 2–4 to analyse the collective coverage and impact, study contribution type, as well as its evaluation technique based on our systematic review. However, in the work of (Opara-Martins et al. 2016), RQ.IV and RQ.V have already been answered and critically discussed as per the vendor lock-in problem in the cloud environment. This referenced work discuss the different strategies and standards to avoid vendor lock-in risks in cloud migration, including the potential of DevOps tools to tackle the cloud lock-in problem (i.e. addressing RQ.V).

4.0 Results and Discussions

In this section, we summarise the results of this systematic review based on the initial RQ.I – RQ.III. Since, it is crucial to communicate the results of our study effectively to influence enterprise IT decision-makers, managers, and cloud practitioners, thus we specify the dissemination strategy in this review extends beyond academic journals and/or conferences to include practitioner-oriented journals and magazines (refer to Opara-Martins et al. 2017). Herein, we discuss the answers to our review question(s).

4.1 *RQ. I What are the associated risk factors of vendor lock-in affecting enterprise migration to cloud computing SaaS environments?*

For cloud computing to achieve its potential, there needs to be a clear understanding of the various vendor lock-in challenges involved. While a lot of research is currently taking place in the technology itself, there is an equally urgent need for understanding the technical, legal, and business-related issues of vendor lock-in surrounding cloud computing. Within this work, we have initially targeted the switching difficulties and lock-in challenges of migrating between cloud SaaS vendors (whether public, private or hybrid ones). The option of switching and/or changing cloud service providers is a key right for cloud service consumers and enterprises. Unfortunately, many enterprise decision makers are in no position to realise this valuable opportunity to save cost by retaining the flexibility to change cloud providers to suit the organisational needs. Instead, they are burdened by the oversized, complex migration and costly integration and porting effort to handle. Thus, the gap between what the business needs and expects (in terms of switching), and what its IT group can deliver, continues to grow wider. To bridge this gap, we identify the need to examine various barriers that enterprises and cloud consumers may encounter when switching between cloud services and/or vendors in the SaaS marketplace. Based on the review of existing literature studies and the results extrapolated from **Table 3**, the following constraints and challenges have been identified with switching between cloud SaaS vendors: switching cost, data portability, API propagation and integration issues, interoperability and standards, security risks, contract and SLA management, and legal challenges (data location constraints, data ownership rights, cloud in/exit issues, legal jurisdiction and compliance etc.). They have been further grouped into three main challenge (i.e. technical, business environment, and legal) areas of SaaS migration, and briefly analysed below. This grouping is based on assigning the single most applicable cloud migration topic-category to a group of related subcategories (e.g. subtopics 'Integration issues', 'API propagation', 'Technical incompatibilities' etc. were grouped into a higher-level topic 'Technical Challenges'). Each subtopic was assigned to individual articles (using Sn) according to the articles' specific research interest. It is inevitable that a piece of research may contribute to several of the subcategories.

Therefore, to systematically reveal and examine academic insights on cloud computing migration challenges, a literature classification scheme was developed. This classification was based on categorizing the research focus of the 64 selected articles. Specific subcategories were assigned to each article and then synthesized into more generic top categories in three main challenge areas described below. The categorisation of the first four grouped challenges are technical constraints related to the growth (i.e. in terms of migration to, and adoption) of cloud computing SaaS services, the next four are internal business environment obstacles to switching between cloud vendors once the SaaS solution has been and/or replaced, and the last four challenges are policy and legal issues intrinsic to cloud SaaS migration process. These challenges represent shared concerns that need to be addressed prior to SaaS adoption, or switching between cloud SaaS service and vendors. They have been listed out and presented in a tabular form (refer to **Table 4**) along with the classification description, study reference number and citation impact to show the representativeness of each category in the total amount of references identified. In doing so, we employed a quantitative approach to identify the number of references dealing with each challenge area of SaaS lock-in, to raise awareness of the core cloud migration risk factors which have received more attention and support in the research community and those of which have not been so extensively analysed (see **Figure 2**).

Table 3. Categorisation of Cloud Lock-in Challenges impeding SaaS Migration

Migration Challenges	Description	Study ID [Sn]	Count
Technical Challenges	Integration issues	[S7, S11, S40, S47, S9, S12, S14, S16, S25, S32, S47, S52, S55, S56]	14
	API propagation	[S7, S12, S14, S16, S32, S55]	6
	Technical incompatibilities	[S2, S3, S4, S16, S31, S37, S45, S46, S47, S51, S55]	11
	Data and application compatibility issues	[S3, S4, S9, S11, S16, S18, S29, S31, S32, S34, S37, S47, S52, S54]	14
Business Environment Challenges	Interoperability and standards	[S5, S7, S11, S16, S32, S35, S45, S53, S54, S55]	10
	Data portability issues	[S5, S7, S11, S16, S18, S32, S35, S37, S45, S53, S54, S55]	12
	Security risks	[S7, S10, S11, S43, S42, S51, S56, S63]	8
	Switching costs	[S26, S32, S37, S47, S52]	5
Legal Challenges	Exit strategy	[S15, S32, S25, S47, S52]	5
	Contract and SLA management	[S15, S17, S52, S56]	4
	Data preservation and governance issues	[S10, S41, S47, S52, S63]	5
	Legal jurisdiction and compliance risks	[S15, S40, S42, S51, S52, S56]	6

A. **Technical Challenges**: This category focuses on technology details of cloud computing. Articles in this category are published by researchers who consider cloud computing services to be plug and play systems, and are interested in its component and mechanisms that support interoperability and portability. With the growing availability of many new SaaS offerings, companies desire common integration methods and services to support agility and the rapid proliferation of new capabilities. In this aspect, we describe related challenges of lock-in that affects (i.e. constrains) core elements necessary for the smooth implementation, configuration, operation, and migration of a cloud SaaS service for enterprise adoption. Particularly, we report on how different API categories and interface types (i.e. whether standard or proprietary) can either trigger or reduce lock-in risks by offering seamless integration and compatibility within and between multiple cloud SaaS vendors, and with the enterprises internal IT system(s).

B. **Business Environment Challenges**: This category concerns the business implications of cloud computing. The articles in this category treat cloud computing as a black box technology which can generate business value to both providers and customers. The issues described herein are necessary to trigger a SaaS lock-in in the business context. They are discussed to encourage consistent mechanisms to enable cloud consumers and enterprises to quickly and efficiently consume SaaS by standardising interactions between cloud customers and cloud vendors. These include specifications and agreements on data and metadata formats, or on standards for interoperability, portability and security. In other words, the challenges in this category are necessary elements for the support of cloud computing activities within already existing enterprise IT infrastructures for which technology neutrality is a necessity.

C. **Legal Challenges**: This category contains articles that provide a general overview of cloud computing legal challenges for enterprise adoption, with an aim to provide general understanding of this area per the vendor lock-in problem, rather than to focus on any specific legal facet. The categorisation of legal issues includes related challenges with contract, software licenses, exit process or termination of the SaaS solution in question, judicial requirements and law. The following legal challenges of lock-in described below are crucial constraints worth considering for enterprises with strict governance policies and regulatory (compliance) obligations, as they move data and application services across cloud SaaS environments.

Figure 2 depicts the results obtained for the number of citations on cloud SaaS migration issues. Grouping the challenges using the categories explained earlier leads to the construction of **Figure 2**, which shows that legal challenges arising from a cloud lock-in scenario represents a lesser minority with 20% of citations covered. This finding reveals the need for further research on legal and political aspects of lock-in risks such as exit strategy, contract and SLA management, data preservation and governance issues etc. However, also in **Figure 2**, we can see that technical (45%) challenges and business challenges (35%) respectively represent a clear majority of problem references. In other words, these challenges are highly relevant to overcoming vendor lock-in risks in the cloud but there is still considerable ambiguity with regards to the studies proposing solutions for tackling them. A conclusion that could be drawn from this analysis is that, although these technical and business challenges (as listed in **Table 3**) are significant barriers to cloud migration and adoption by enterprises, yet little is available in terms of research articles and industry reports with solutions to these problems. For instance,

when analysing the number of citations for the associated elements of vendor lock-in using the description in **Table 3**, we can see the two major challenge areas of vendor lock-in identified in these references are technical- and business environment-related issues.

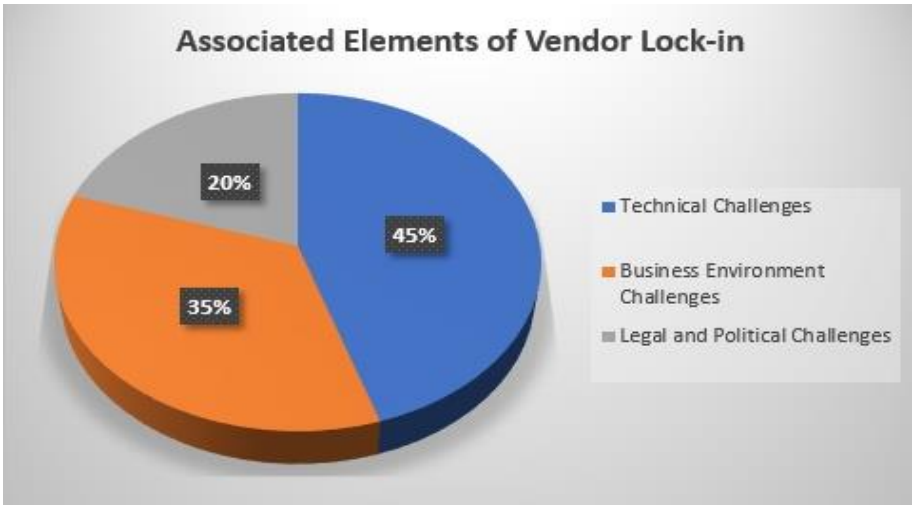


Figure 2. Pie Chart for Problem Citation

As an example, integration, data portability, and incompatibility issues for instance are three main lock-in risk factors mentioned and discussed in several of the referenced studies, as also indicated in **Table 3**. This is because as new cloud SaaS services are deployed within an existing enterprise environment the need to integrate them with various on-premise systems and other cloud services becomes important. There are many causes of potential incompatibility between different cloud providers that could also arise while trying to transfer an application or data across different environments (Gonidis, 2013). Thus, integration task and the need to ensure data portability has increased the complexity of decision-making in respect of enterprise cloud SaaS migration (Opara-Martins et al. 2015; Adel et al. 2014; Dillion et al. 2010; Gao et al. 2011; Cusumano 2010). Therefore, as organization's struggle with the complexities of integrating cloud services with other critical systems residing on-premise, the ability to share data (i.e. portability) across these hybrid environments remains critical, and continues as more enterprise workloads (i.e. an independent service or collection of code that can be executed) and projects are committed to cloud computing SaaS services. However, depending on the type of workload, the migration and/or porting effort will be lower than others. Therefore, to allow the easy use of cloud SaaS systems and to enable the migration of applications and data between the SaaS offerings of different cloud providers, there will be the need for a standardized cloud API (Opara-Martins et al. 2017a). But, there is no commonly agreed-upon API or cloud reference implementation that developers, programmers, and cloud architects can rely on (Weinhardt et al. 2009). Nonetheless, a standard will be required in the long run to make the vision of the cloud come true, until then cloud service consumers remain susceptible to proprietary vendor lock-in risks.

While **Figure 2** shows the percentage distribution of studies tackling the vendor lock-in challenges identified in **Table 3**. The least cited element of vendor lock-in highlighted in this table and figure are related to legal challenges. Based on the categorisation of identified challenges and review of related studies in this aspect, the following observation is made; although our systematic literature analysis has revealed that articles focused on the technical challenges of cloud lock-in outnumbered business and legal challenge-focused ones, in our view, these articles do not meet the challenge made by Robey and Markus (1997) more than ten years ago to produce more consumable research. Migration to, and adoption of cloud computing services (SaaS, PaaS, and IaaS) in the enterprise is a major concern in the practitioner community, and in our view, there is an urgent demand for articles explaining cloud computing technologies and especially the vendor lock-in problem in a business-friendly language. Existing articles in the 'technological challenges' category focus mostly on specific technical details which are often addressed from various cloud computing technical specialists' standpoint. These articles may be informative but do not offer much practical or applicable knowledge to business professionals who are on the user side of cloud computing. Business users and legal practitioners may find it extremely difficult to read these articles, digest the knowledge, and envisage the implications to business strategies and practices, even when the topics of the articles (e.g. cloud migration, vendor lock-in, switching costs, security etc.) are highly relevant to business interests.

In addition, the results from **Table 3** also shows that there is an obvious need for more research in the 'legal challenges' category from both cloud computing providers and cloud service consumers' perspective. Such contributions would help in shedding light on the legal obscurity and complications associated with migrating enterprise business systems to operate in the cloud computing environment. Moreover, existing articles in this legal category tend to take a black-box approach when studying cloud computing migration and fail to make nuanced distinctions between different migration types, service layers, and deployment models of cloud computing. Further research should acknowledge the differences across the four migration types, three service layers, and explore the implications for businesses in a subtler manner. Furthermore, being that all the other sub-challenges (e.g. exit strategy, interoperability, portability, switching costs, contract and SLA management) under the 'Business and Legal Challenges' category contribute in varying degrees to the decision-making process for migrating and/or adopting cloud computing services. However, there are many other research opportunities beyond 'migration' or 'adoption' for IS scholars interested in cloud computing and vendor lock-in phenomenon. Given that cloud computing potentially represents a paradigm shift in ICT service delivery methods, many traditional ICT management issues with high practical relevance deserve rigorous academic re-examination in the cloud computing context. As an example, these questions could include: How does vendor lock-in challenge(s) in cloud computing impact current practices of IT service management and governance? Does vendor lock-in challenge in cloud computing affect IT business alignment and IT agility? What are the critical factors of a successful migration to a cloud SaaS environment with no risk of vendor lock-in? Mainstream IT, IS and Software Engineering journals, conferences, editorials etc. could encourage further discussions and investigations in these areas.

4.2 ***RQ. II*** *What are the existing tasks, methods, techniques, activities and decisions available to avoid vendor lock-in risks when migrating or switching between SaaS vendors/services and on-premise systems?*

Migration to the cloud is not without pitfalls (Opara-Martins et al. 2016). Therefore, the reasons for the migration and adoption of cloud computing SaaS solutions should be explained to the decision makers as well as to the users (i.e. any person involved should learn how to benefit from the cloud SaaS solution). In this section, we address the review question above by developing and proposing a decision framework to assist IT managers who are determining which cloud SaaS solution matches their specific business requirements and evaluating the numerous commercial claims (in many cases unsubstantiated) of a cloud's value in terms of portability, interoperability, and ease of integration. This decision framework is the result of the authors' comprehensive research program in understanding how vendor lock-in risks can affect enterprise migration and adoption of cloud services. It recommends the appropriate decision step and supporting activities based on the way in which IT is currently used in the enterprise and future needs to meet competitive lock-in challenges. The proposed framework will also help IT managers correctly allocate investments and assess cloud SaaS alternatives that now compete with applications hosted within their in-house data centres. Overall, our decision framework is useful to help inform decision makers about the difficulties (e.g. switching costs, interoperability, portability etc.), benefits and proprietary lock-in risks of using the cloud. In other words, the framework provides a starting point for cloud computing vendor lock-in risk assessment in the enterprise.

To answer RQ.II, the classification of tasks, activities, and decision steps to avoid vendor lock-in risks when migrating or switching between cloud SaaS vendors (and on-premise systems) have been identified and extensively discussed in (Opara-Martins et al 2017a). Note, that the cloud SaaS migration decision steps, tasks, and supporting activities discussed in the referenced work have been identified from selected secondary sources (see reference list) and the primary studies cited in **Table 3**. Together, these studies were analysed in the context of SaaS lock-in (i.e. related migration challenges) and potential solutions by evaluating the number of citations for each referenced study including their overall research contributions. In this regard, we adopt situational engineering method proposed by (Brinkkemper, 1996) to consolidate existing decision support systems and frameworks in cloud migration by exploring the defined migration tasks and decisions in the primary studies. By doing so, we have identified the key decision steps and processes related to cloud SaaS migration scenarios, extracted a list of common migration tasks or supporting activities, and group the closely related tasks in terms of output artefacts to form key decision processes for enterprise cloud SaaS migration. For this purpose, we enrich existing research on cloud computing migration and adoption, and present a systematic approach to assist enterprises assess the risks of vendor lock-in.

4.3 ***RQ. III*** *How is cloud migration reported within existing research theme?*

Now, to specifically answer RQ.III, we conducted a systematic review of existing approaches for cloud (i.e. SaaS-to-SaaS) and legacy to cloud migration. This is done to identify and analyse the vendor lock-in challenges considered in these cloud and/or on-premise migration approaches. Through integral analysis, **Table 3** is

presented to analyse current research contributions and gaps that need to be filled in terms of SaaS cloud migration problems and the possible solutions offered to address the vendor lock-in risks. Note, the study number (abbreviated as Sn) attached to each referenced study are used simply to show the order (i.e. labels), not to show how much better each paper is with others (as in study quality computation for instance). While **Table 3 d**oes not aim to provide a critique on the existing cloud migration approaches, however it does present a broad understanding of what essential activities and concerns are involved during the cloud-to-cloud or legacy-to-cloud migration process. Therefore, as shown in **Table 3**, our review is based on 64 different studies on cloud migration which primarily focuses on the technical rigor of content presented. The nominated journals and conferences are shown in the following **Table(s) 4–6**, whereas the distribution of studies per their publication year (refer to **Figure 3**), contribution type, and evaluation method is presented using pie charts (see **Figure(s) 4–5**) to show the representativeness of each category/group in the total of references identified. Together, these studies were analysed in the context of SaaS lock-in (i.e. related migration challenges) and potential solutions by evaluating the number of citations for each referenced study including their overall research contributions. In the following sub-sections, we analysed the articles by year of publication, the publication outlets, active research communities and institutes, geographical distribution of studies, primary contribution, and evaluation methods.

Table 4. Distribution of Publication per Citation Value

Year	Publication Count (Pc)	Percentage value (Pv)	Citation Value (Cv) per Year
2010	12	18.8%	18407
2011	**19**	29.7%	1601
2012	10	15.6%	772
2013	13	20.3%	712
2014	4	6.3%	55
2015	2	3.1%	11
2016	3	5%	19
2017	1	1.6%	1
Total	**64**	**~100**	**21578**

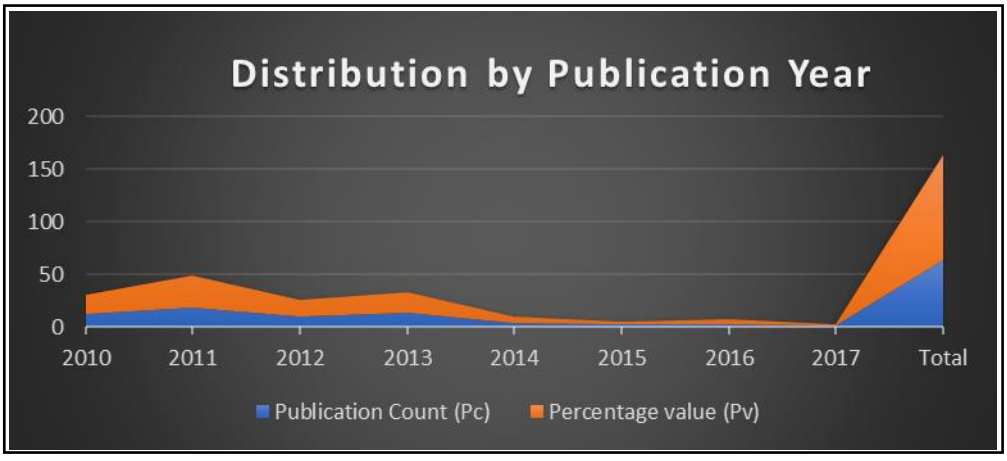


Figure 3. Distribution by Publication Year

4.3.1 Frequency by Publication Year

Figure 3 shows the graphical distribution in the number of studies by year of publication. Percentage value (abbreviated as Pv) represents the estimated proportion in the total number of publications per year. The percentage values are given in parenthesis. Citation value (abbreviated as Cv) shows the total number of citations for each publication year. This number has been added up together at the end of each year to give the actual citation value in each publication year. The citation rates for the included studies were obtained from Google Scholar. The citation rates of the studies are quite high (for most studies between 2010 and 2013), but it suddenly dwindles down from 2014 to 2017. This result is in line with common expectations since the initially selected studies were published from 2010 to 2017, and 16% of those that were eventually included were published in last four years. According to Google Scholar data, the most cited publications from our selected set of studies are [S9] with 13065 citations and [S49] with 2294 citations (refer to Table 3). When the year of publication of the papers is concerned (Figure 3), we noticed an inverse trend in the number of relevant

publications about cloud computing and vendor lock-in risks. As shown in Figure 3, from 2010 to 2017 the number of peer-reviewed articles has decreased substantially. Considering 2017 in the figure represents only half a year worth of publication count, we can predict the total number for that year will easily exceed that of 2016. This implosion of publications reflects the immaturity of cloud migration and vendor lock-in research. Thus, this calls for further work in this direction on fostering industry and academia's increasing acceptance of vendor lock-in problem in cloud computing migration as a salient and legitimate research area. Moreover, the results in Table 4 presents the frequency of the selected studies and their citation values since 2010. The earliest research study considered in our review are published in the year 2010 to 2017 (with the least number of publication count). Note that for 2017, the review only considered cloud migration and vendor lock-in research studies until April. Perhaps, that explains the reason for the funnelled decreased in the number of publication (i.e. 1.6%) and citation count (i.e. 1) in 2017. Publication count (abbreviated as Pc) in Figure 2 and Table 4 respectively, shows the number of publications per year. As an example, we annotate 2011 as the year with the most Pc with 19 papers (29.7%) followed by 2013 with 13 cited studies (20.3%). As presented in this table, there has been a continuous decline in the number of publications from 2014 to 2017.

4.3.2 Distribution by Publication Type

The publication channels of the articles were also analysed. Among the 64 included studies, **Table 5** presents a classification of publications from academia and industry sectors. It indicates that most of the contributions are related to conferences with 32 (50%) publications out of all 64 selected primary studies. The selection of studies used in this classification are listed in **Table 3**. Most cited studies have been published in five Services conference, three IEEE and IARIA cloud computing, grid and virtualisation conferences and two European conference on Software Maintenance and Reengineering (CSMR). The second ranked publication channel is journals with 18 (28.1%) publications in total. Among them, Elsevier journal of *Systems and Software* and Springer *Journal of Cloud Computing – Advances, Systems and Applications* published the most papers (i.e. 2 respectively) related to cloud computing migration and SaaS lock-in challenges. Workshops (15.6%), book chapters (4.7%), and industry reports (1.6%) are ranked as third, fourth and fifth regarding the publication count and percentage value of total publications, respectively. However as indicated in **Table 5**, ACM workshop on *Software Engineering for Cloud Computing* and IEEE workshop on *Maintenance and Evolution of Service-Oriented and Cloud-based Systems (MESOCA)* have the highest number (i.e. 3 and 2 respectively) of publications per channel. The active research communities with at least two or more included studies are listed alongside their research focus in **Table 6**. Based on these findings, overall, it can be observed that most of the included studies in Table 5 are published in cloud computing, virtualisation, service-oriented computing and software engineering communities. This observation, however, is consistent with the findings of a recently conducted systematic review study on cloud migration research by (Jamshidi et al. 2013). **Table 5** is a helpful resource for academic and industry researchers wanting to publish cloud computing studies or for anyone within this field looking for good quality practitioner-oriented outlets and cloud-computing references.

Table 5. Distribution of Studies per Publication Channel

	Publication Channel Name	Publisher Name/Acronym	Publication Count (Pc)
Journals	Springer Journal in Computing	Springer	1
	Journal of Internet Services and Applications	Springer	1
	ACM Computer Communications Review	ACM SIGCOMM	1
	Journal of Systems and Software	Elsevier	2
	Information Systems Research Journal	ACM	1
	Software Practice and Experience	Wiley Online Library	1
	Journal of Software, Evolution and Process	Wiley Online Library	1
	IEEE Transactions on Engineering Management	IEEE	1
	IEEE Transactions on Cloud Computing	IEEE	1
	International Journal of Automation and Computing	Springer	1
	European Journal of Law and Technology	Warwick University	1
	Journal of Cloud Computing: Advances, Systems and Applications	Springer	2
	Journal of Information Technology Management	University of Baltimore	1
	Communications of the ACM	ACM	1
	Future Generation Computer Systems	Elsevier	1
	ACM SIGPLAN Journal	ACM	1
		Total	***18 (28.1%)***

	Publication Channel Name	Publisher Name/Acronym	Count
Conferences	European Conference on Service Oriented and Cloud Computing	Springer	1
	World Congress on Services	IEEE	5
	International Conference on Algorithms and Architectures for Parallel Processing	Springer	1
	International Conference on Cloud Computing, GRIDS, and Virtualisation	IARIA (International Academy, Research, and Industry Association)	3
	International Conference on Cloud Computing (CLOUD)	IEEE	3
	International Conference on Advances in Computing. Communications and Informatics	ACM	1
	International Conference on World Wide Web (WWW)	ACM	1
	International Conference on Digital Ecosystems and Technologies	IEEE	1
	USENIX Conference on Hot Topics in Cloud Computing	ACM	1
	International Symposium on Symbolic and Numeric Algorithm	IEEE	1
	European Conference on Software Maintenance and Reengineering (CSMR)	IEEE	2
	International Conference on Information Society (i-Society)	IEEE	1
	International Conference on Cloud Computing and Service Science (CLOSER)	SciTePress	1
	International Conference on System Sciences	IEEE	1
	International Conference on Grid Computing (GRID)	IEEE/ACM	1
	International Conference on Trust, Security and Privacy (TrustCom)	IEEE	1
	Conference on e-Business, e-Services and e-Society	Springer	1
	International Conference on Advanced Information Networking and Applications	IEEE	1
	European Conference on Information Systems	AIS Electronic Library (AISeL)	1
	International Conference on Cloud Computing Technology and Science (CloudCom)	IEEE	1
	International Conference on Service-Oriented Computing and Applications (SOCA)	IEEE	1
	ACM SIGMETRICS on Performance Evaluation Review	ACM	1
	International Conference on Current Trends in Theory and Practice of Informatics	Springer	1
		Total	***32 (50%)***
Book Chapters	**Publication Channel Name – Book Chapters**	**Publisher Name/Acronym**	**Count**
	International Conference on Cloud Computing (CloudComp)	Springer	1
	European Conference on a Service-Based Internet	Springer	1
	Oracle Client/Server Modernization	Elsevier	1
		Total	***3 (4.7%)***
Workshops	**Publication Channel Name**	**Publisher Name/Acronym**	**Count**
	International Workshop on Software Engineering for Cloud Computing	ACM	3
	arXiv Preprints	Cornell University	1
	International Workshop on Maintenance and Evolution of Service-Oriented and Cloud-Based Systems (MESOCA)	IEEE	2
	Workshop on Software Engineering for Cloud Computing	ACM	1
	Springer-Plus Journal	Springer	1
	International Conference on Modelling in Software Engineering	IEEE	1
	Workshops on Service-Oriented Computing (ICSOC)	IEEE	1
		Total	***10 (15.6%)***
Industry Reports	**Publication Channel Name**	**Publisher Name/Acronym**	**Count**
	NIST Special Publication	NIST	1
		Total	***1 (1.6%)***
	Total of all Publication Type:	**64**	***100%***

4.4 What evaluating procedures have been used to assess the results in each paper?

In this section, before presenting the evaluating procedures, we first discuss our findings by grouping the cited studies according to their contribution type. We use the descriptions presented in **Table 9** to group the selected studies in **Table 3** according to their contribution type and the evaluation method used within each cited article.

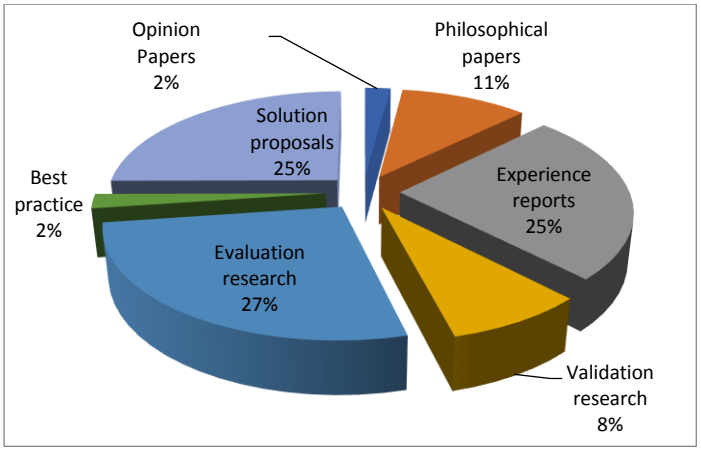
Table 9. Description of Extracted Data Items from Table 3

	Options	**Description**
Study Contribution Type	Opinion papers	A cloud computing research study that reflects author's opinion in migration and vendor lock-in problem.
	Philosophical papers	A cloud computing migration study that investigates a new way of doing and/or looking at things e.g. a new framework for migration to cloud computing environments.
	Experience reports	The experience may concern one migration project or more, but it must be the author's personal experience. Such study should contain a list of lessons learnt.
	Evaluation research papers	A cloud computing research paper that investigates a problem (e.g. vendor lock-in, interoperability, portability, integration etc.) in migration practice or an implementation of a migration technique in practice.
	Best practice	A research study comprising of approaches reporting best practices of migrating cloud and/or on-premise enterprise business applications and data from one cloud provider to another.
	Solution Proposals	A research study that proposes a novel method, technique or frameworks and argues for its relevance. A proof of concept may be offered as a solution in such studies.
	Validation research	A study that investigates the properties of a solution that has not yet been implemented in migration practices. This solution may have been proposed elsewhere.
Evaluation Procedures	Survey reports	Exhaustive survey of the state-of-the-art of cloud migration approaches to provide evidence for evaluation and validation.
	Experience and lessons learned report	Personal experience of the author(s) and lessons learned to communicate to cloud and IT practitioners. Note, the experience may concern one or more migration cases and the lessons learned in real-world cloud migration projects.
	Controlled experiment	Experimental investigation of a testable hypothesis, in which conditions are set up to isolate the variables of interest and test how they affect certain measurable outcomes.
	Proof of Concept (PoC) Example	Research papers that encourages enterprises to adopt and migrate to cloud-based services for mission and non-mission critical systems and to undertake proof of concept studies to fully understand the risks (e.g. vendor lock-in, interoperability and portability) of cloud computing. Toy and small PoC examples.
	Case study	A technique, procedure, or method for detailed exploratory investigations that attempt to understand and explain phenomenon or test theories, using primarily quantitative analysis.
	Mathematical proof	A demonstration that if some fundamental statements (axioms) are assumed true, then some mathematical statement is necessarily true.

4.4.1 Distribution by Contribution Type

Amongst the list of studies cited in **Table 3**, we considered it useful to identify what type(s) of research contributions are dominating these publications, before presenting the evaluation techniques used within the study. In doing so, we analysed the distribution of papers by research contribution type, as shown in **Figure 4**. According to this figure, "evaluation research", "solution proposals" and "experience reports" dominate the publication population with 13, 12, and 12 number of research papers (i.e. 27%, 25%, and 25% of all publications), respectively. On the other end of the scale, there are only 5 number of philosophical papers (i.e. 11% of all publications), 4 number of validation research (i.e. 8% of all publications), and just 1 best practice research study (i.e. 2%% of all publications) studies. However, it can be observed that there is only 1 "opinion papers", perhaps this type(s) of research contributions are either not popular nor has it been widely accepted by the cloud computing community. Further interpretation of the shortage of philosophical papers may also indicate that there is a lack of theory building work in cloud computing research and vendor lock-in challenge. However, since "validation research", "evaluation research", and "solution proposal" research contribution types can be grouped into empirical research, hence our systematic review have hitherto identified that there is a vast gap in

theoretical research approaches for cloud computing migration. Besides, the amount of papers in the "Experience report" category indicates a significant participation by practitioners in cloud computing research. This is an important finding in terms of bridging existing research gap (among academia and industry) in current cloud computing publication outlets (i.e. conferences, journals, workshops etc.). To substantiate, for instance, we noted that the contributions on experience reports are predominately made by collaboration between researchers from the industry and academia (this information was obtained from the author affiliation details of the papers cited in **Table 3**). This finding is extremely positive, as it demonstrates that the studies included in our review have a strong industry engagement.

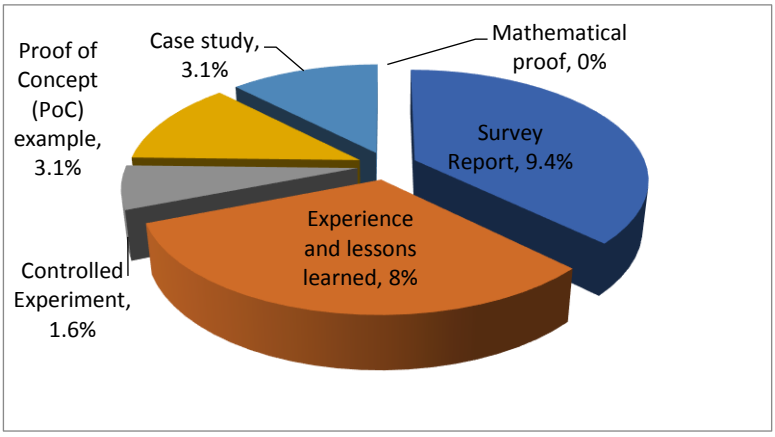


Contribution Type	Study ID
Opinion Papers	[S39]
Philosophical papers	[S5, S10, S16, S22, S58]
Experience reports	[S1, S3, S12, S18, S26, S28, S29, S35, S36, S47, S49, S62]
Validation research	[S2, S41, S51, S55]
Evaluation research	[S8, S14, S25, S32, S33, S40, S43, S46, S50, S52, S54, S61, S64]
Best practice	[S42]
Solution proposals	[S6, S7, S13, S15, S17, S20, S21, S34, S48, S56, S57, S63]

Figure 4. Pie Chart for the Distribution of Studies per Contribution Type

4.4.2 Distribution by Evaluation Technique

Figure 5 analyses the distribution of papers by evaluation methods. As shown in this figure below, we can conclude that surveys (9.4%), experience and lessons learned (8%) are the most common evaluation method adopted by cloud computing researchers. However, the PoC example (3.1%) and case study (3.1%) approach was also seen to be common amongst cloud researchers cited in this review study. A lesser minority of adopted the controlled experiment evaluation approach. In terms of comparison, we deduce that controlled experiments (1%) are known to support quantitative analysis and scientific investigation of a specific cloud migration approach (e.g. Type I, Type II, Type III, and Type V), lock-in challenge area (e.g. technical, business, and legal) and cloud deployment model, but ignore contextual factors and real situations. Whereas, surveys and case studies on the other hand, are good evaluation techniques for real-world cases and effects. Additionally, % of studies used PoC toy examples to evaluate their contributions. Nonetheless, as **Figure 5** indicates, there is a clear lack of research evaluation methods based on mathematical proofs (0%).



Evaluation Method	Study ID
Survey Report	[S9, S31, S38, S44, S45, S59]
Experience and lessons learned	[S11, S19, S23, S24, S37]
Controlled Experiment	[S27]
Proof of Concept (PoC) example	[S30, S60]
Case study	[S4, S53]
Mathematical proof	0

Figure 5. Pie Chart for the Distribution of Studies per Evaluation Method and Type

4.5 Implication of Key Findings

In summary, there is no single solution to the SaaS lock-in problem in the cloud, since the choice of method for migration depends on the goals (i.e. reasons for organisations to migrate to cloud-based environments), the available budget and resources and the time needed to complete the initial migration project (Almonaies et al. 2010). Thus, the decision to migrate/replace enterprise systems to/with a cloud computing SaaS solution involves several technical and infrastructural changes in the on-premise enterprise IT environment, such as data repositories movement, application and network infrastructure configuration, application evolution and redeployment (Andrikopolous et al. 2013). For this reason, SaaS application developers must carefully consider possible technical restrictions that may hinder interoperability and portability, (or even avoid) cloud adoption by the organization, such as when its source SaaS (or legacy) applications may violate environmental constraints imposed by the target cloud provider (Frey et al. 2013). From a holistic perspective, such problems are often attributed to the social-technical/economical aspects of vendor lock-in. Moreover, another challenge in this direction consists of modifying or adapting a SaaS application such that it can benefit from the cloud services and resources, such as replacing a relational database by a cloud-based NoSQL one, an adaptation known as cloudification (Mendoca, 2014; Andrikopolous et al. 2013). Such adaptation techniques in the cloud SaaS environment lead to challenges such as incompatibilities with the database layer previously used before migration, and the characteristics of an equivalent database layer hosted in the cloud – with respect to the semantics of the database schema and/or the database name. With respect to data and application incompatibility resolution in the cloud SaaS environment, Gholami et al. (2016) discussed different existing adaptation mechanisms that might be required to resolve incompatibilities. Therefore, migration to SaaS cloud environment requires to consider the specific migration strategy per the legacy system and existing SaaS solution. If existing SaaS solution has the same business functionality of legacy system, for example, users can replace legacy system by SaaS. Whereas, when some business functionality has been realised by existing SaaS, legacy system can be modernised by revising legacy system based on existing SaaS alternatives (Zhao and Zhou, 2014). Furthermore, as pointed out by (Almonaies et al. 2010), it is not always straight-forward to reuse legacy components and expose them as SaaS cloud services as it might impose a higher lock-in risk for business-critical systems and a higher switching (or porting) cost for enterprise systems than replacing them entirely with a cloud-native SaaS application.

4.6 Threats to Validity

Within this work, we have identified two main threats to the validity of our systematic review, namely: publication bias and single researcher data extraction threats. The first refers to the problem that positive results are more likely to be published than negative results. Due to our initial research problem, we focused this systematic review on studies whose primary objectives was to suggest an approach (i.e. systematic methodology, framework or decision support) for tackling the vendor lock-in challenges affecting enterprise cloud migration and adoption, specifically in the form of a decision framework. What this implies is that we may have missed some relevant studies, and thus underestimate the extent of cloud-related research. Particularly, we will have missed articles published in conferences aimed at specific IT management and software engineering topics which are more likely to have addressed review questions rather than research trends. Additional challenge in addressing these threats was to determine the scope of our study, since cloud migration and vendor lock-in relates to different communities including software engineering, information systems and networks. However, to reduce this threat by ensuring the process of publication selection was unbiased, we developed a review protocol. Moreover, as pointed out by (Iankoulova and Daneva, 2012), the challenges to an unbiased systematic review study are that there is no single publications' source, the literature is fragmented and not everything can be accessed online. To reduce the bias further, more literature search could be done throughout publications that are not written in English (note, this could also affect the inclusion and exclusion criteria for selected study).

The second threat means that some of the data we collected may be erroneous since data extraction was performed independently by the first author. However, a detailed review of other systematic literature reviews has suggested that the extractor/checker mode of working can lead to data extraction and aggregation problems when there are many primary studies or the data is complex (Turner et al. 2007). Nonetheless, in this

quantitative study, there were relatively few primary studies and the data extracted from the selected articles were relatively objective, so hopefully this will reduce the likelihood of erroneous results. Finally, we acknowledge that even though systematic reviews are generally reliable (Zhang and Babar, 2013), still there exist some potential limitations with this type of study. One potential limitation worth mentioning here is that, our sample was mainly dominated by academic publications. As cloud computing is industry-driven in nature, many quality professional articles may also embrace this phenomenon. Thus, may hinder the ability of the present article to present a complete picture of the current developments in this domain. Another possible limitation noted in this systematic review is that our access to relevant sources is dependent on the appropriateness of the search strings used. In addition, the keywords used to retrieve literature may well be extended to the fields of grid computing, parallel computing, SOA and distributed computing migration which are tightly related to cloud computing migration approaches and challenges.

5.0 Conclusion

This appendix has discussed the SaaS lock-in challenges that may limit the viability of cloud computing for enterprises where portability, interoperability, standards and security control over proprietary information concerns are key to competitive success and efficient operation. Researcher analysed these concerns through three categories of migration decisions, and present a decision framework with the types of challenges decisions that enterprises should consider in deciding to move wholly or partially to a cloud computing SaaS environment.

Practitioner and academic interest in the evolving vendor lock-in phenomenon of cloud computing is intense. While this systematic literature review cannot claim to be exhaustive, however it provides insights into the current state of cloud computing migration research. This appendix presented a systematic review on the cloud-to-cloud and legacy-to-cloud migration process from a decision-making framework perspective. The objective of this review is to identify, analyse and classify existing challenges of vendor lock-in affecting enterprise migration to cloud SaaS environments. By doing so, researcher portrays a current landscape of vendor lock-in and cloud computing migration research stream, where it is today, and most importantly, given the current relevance of the topic, some suggestions as to where more effort should be focused in the future to produce more 'consumable research'. In contrast to existing works, this study extends the scope of cloud computing migration beyond one specific challenge areas, addressing vendor lock-in from three main perspectives or categories (i.e. technical, business and legal). As far as the initial RQ.I – RQ.III is concerned, author reviewed and evaluated existing approaches and research contributions to give answers to this review question(s) grouped into three categories: 1) Vendor lock-in risk identification, analysis and classification, 2) Identification and analysis of active research communities, fora, and institutes concerned with cloud computing migration and vendor lock-in research, and 3) Gap analysis and maturity level of the cloud SaaS migration research contributions. The first set of questions was used to build a thorough understanding of the work carried out to solve known cloud lock-in, portability and interoperability problems. The second question set was used to assemble a detailed map of current research in the area. Finally, the last set of questions underpinned the identification of gaps in the current solutions. By doing so, we can summarise the contributions made by this study as follows:

- To help researchers (i.e. academia) and practitioners (i.e. industry) in the cloud computing community have a deep understanding of the current state of cloud computing (SaaS) migration approaches proposed in literature, associated vendor lock-in challenges and limitations, as well as understand insightful findings and recommendations to be learned.
- To provide a comprehensive view of cloud SaaS migration challenges, specifically concerned with decision frameworks, tools, and processes for cloud-to-cloud migration and legacy-to-cloud migration (or vice-versa), that need to be investigated further – hence a prelude to further research activities can be opened.

Therefore, the adopted methodology allowed author to classify/categorise, from different perspectives (e.g. technical, business etc.), the main vendor lock-in risk factors for cloud SaaS migration, and taking into consideration crucial security and legal challenges (e.g. data ownership, portability, exit strategy etc.). This methodological approach resulted on a comprehensive analysis of selected cloud migration research studies

provided as basis for analysis, hence promoting the need of a decision framework to avoid vendor lock-in risks for adoption and migration to cloud computing. To summarise, the proposed framework describes what to do when deploying interoperable, portable, and secure enterprise cloud SaaS services, whereas the workflows, questionnaires and reference implementation and supporting strategies details how to do it. All these instruments are to be collectively used by enterprises organisations and public consumers, to define and implement vendor-neutral interoperable and portable cloud-based services.

Future Research Directions

The lack of solid theoretical foundations has long been a concern for cloud computing researchers, IT practitioners and IS academics as reported within this work. This is because of a traditional view that the academic legitimacy of a research field hinges on the presence or absence of core theories. However, IS researchers have recently argued that to increase the legitimacy of an 'applied research' field like cloud computing, relevance to praxis can and should be placed at the centre. Salience and strong results should be major determinants of the academic legitimacy of the IS research field. Cloud computing clearly has salience. Producing strong research results related to praxis may be a natural way to strengthen the legitimacy of the cloud computing research area. It would be interesting to explore whether there is a 'research cycle' associated with the emergence and widespread commercialisation of new technology affordances and innovations, and whether research in cloud computing is following a similar pattern to that of other major technology innovations. The results show that although current cloud migration research is still skewed towards technological issues of vendor lock-in, new research themes regarding social, political, legal and organisational implications are emerging. This review provides a reference source and classification scheme for IS researchers interested in cloud computing, and to indicate under-researched areas of cloud lock-in problem as well as future directions.

As expected, new IT solutions based on cloud computing technologies will need to be robust before they can be widely adopted for mission-critical applications. Early business applications are frequently experimental, and disruptive changes in business models are not always apparent as they are occurring, but only with the benefit of hindsight, once they have stabilised. Thus, it is difficult to predict whether the widespread availability of cloud computing services' will significantly alter the patterns of adoption, migration and diffusion of new cloud-based innovations and result in new business models. However, the research community should be ready to critically examine the issues of vendor lock-in identified within this paper, not merely to report and explain their occurrence after the event, but to offer best practice (i.e. experience reports and lessons learned) to combat such hurdles in the future when migrating to the cloud environment. This descriptive systematic review provides a useful quality reference source for academics and practitioners with an interest in cloud computing, and suggestions for future lines of research that will have strong salience to IT practitioner community.

Table 3. Categorisation of Selected Primary Studies

Study ID	Authors/Paper Title	Year of Pub.	Migration Type	Unit of Migration	Cloud Deployment Model	Study Contribution Type	Publication Channel	Citation Impact: *Years Covered (2010 – 2017)*
[S1.]	Pahl C et al.**" A comparison of on-premise to cloud migration approaches."**	2013	All	Whole application stack	SaaS, IaaS, PaaS	Experience report and lessons learned	Springer Berlin Heidelberg. In European Conference on Service-Oriented and Cloud Computing Sep 11 (pp. 212-226).	21
[S2.]	Babar and Chauhan **"A tale of migration to cloud computing for sharing experiences and observations."**	2011	Type I, III and IV	Whole application stack	SaaS, IaaS	Controlled experiment	ACM Conference on Computer-Human Interaction. In Proceedings of the 2nd international workshop on software engineering for cloud computing May 22 (pp. 50-56). ACM.	76
[S3.]	Andrikopoulos et al. **"How to adapt applications for the cloud environment**."	2013	All	Whole application stack	SaaS, PaaS, IaaS	Evaluation research	Springer Journal in Computing. Jun 1;95(6):493-535.	135
[S4.]	Mohagheghi and Sæther **"Software engineering challenges for migration to the service cloud paradigm: Ongoing work in the remics project."**	2011	All	Whole application stack	SaaS	Validation and evaluation research.	IEEE World Congress on Services. Jul 4 (pp. 507-514). IEEE	63
[S5.]	Buyya et al.**" Intercloud: Utility-oriented federation of cloud computing environments for scaling of application services."**	2010	Type I, III	Whole application stack	IaaS, PaaS	Philosophical papers	Springer Berlin Heidelberg. In International Conference on Algorithms and Architectures for Parallel Processing May 21 (pp. 13-31).	856
[S6.]	Frey and Hasselbring "**Model-based migration of legacy software systems to scalable and resource-efficient cloud-based applications: The cloudmig approach**."	2010	Type I, III and IV	Whole application stack	IaaS, PaaS, SaaS	Solution proposal	In Cloud Computing 2010: Proceedings of the 1st International Conference on Cloud Computing, GRIDs, and Virtualization.	39
[S7.]	Tran et al. **"Application migration to cloud: a taxonomy of critical factors"**	2011	Type I, II	Whole application stack	IaaS, PaaS	Solution (i.e. framework) proposal	ACM Conference in Proceedings of the 2nd international workshop on software engineering for cloud computing May 22 (pp. 22-28). ACM.	51
[S8.]	Khajeh-Hosseini et al.**" Cloud migration: A case study of migrating an enterprise it system to IaaS."**	2010	Type III	Whole application stack	IaaS	Evaluation research	IEEE 3rd International Conference in Cloud Computing (CLOUD). 2010 Jul 5 (pp. 450-457). IEEE.	309
[S9.]	Zhang et al. **"Cloud computing: state-of-the-art and research challenges."**	2010	Not specified	Virtual machine	IaaS, PaaS, SaaS	Survey and review study	Journal of internet services and applications. May 1;1(1):7-18.	2294
[S10.]	Srinivasan et al. **"State-of-the-art cloud computing security taxonomies: a classification of security challenges in the present cloud computing environment."**	2012	Not specified	Organisation	In general,	Philosophical papers	ACM Conference. In Proceedings of the international conference on advances in computing, communications and informatics Aug 3 (pp. 470-476). ACM	69
[S11.]	Hajjat et al. **"Cloudward bound: planning for beneficial migration of enterprise applications to the cloud."**	2010	Type III	Whole application stack	Hybrid	Experience report and evaluation research	ACM. In Communication Review Aug 30 (Vol. 40, No. 4, pp. 243-254). ACM SIGCOMM Computer	283
[S12.]	Khajeh-Hosseini et al. **"Research challenges for enterprise cloud computing."**	2010	Not specified	Data tier, whole application stack	In general,	Review study	In arXiv preprint arXiv:1001.3257. Jan 19. Cornell University	217
[S13.]	Menzel and Ranjan **"CloudGenius: decision support for web server cloud migration."**	2012	Not specified	Whole Web server migration	IaaS, PaaS	Solution proposal	ACM Proceedings of the 21st international conference on World Wide Web. ACM.	114
[S14.]	Gholami et al. **"Cloud migration process—A survey, evaluation framework, and open challenges. "**	2016	All	All	In general,	Systematic literature review	Journal of Systems and Software. Oct 31; 120:31-69.	6
[S15.]	Alhamad et al. **"Conceptual SLA framework for cloud computing."**	2010	Not specified	Not specified	In general,	Solution proposal	In Digital Ecosystems and Technologies (DEST), 2010 4th IEEE International Conference	176

							on 2010 Apr 13 (pp. 606-610). IEEE.	
[S16.]	Zhu and Zhou **"Research note—Lock-in strategy in software competition: Open-source software vs. proprietary software."**	2012	All	All	IaaS, PaaS, SaaS	Philosophical papers	Information Systems Research. 2012 Jun;23(2):536-45.	43
[S17.]	Khajeh-Hosseini et al. **"The Cloud Adoption Toolkit: Supporting Cloud Adoption Decisions in the Enterprise."**	2010	Type II	Not specified	IaaS	Solution proposal	Software: Practice and Experience.	209
[S18.]	Tak et al. **"To Move or Not to Move: The Economics of Cloud Computing."**	2011	Type I, II and III	Migrate whole application and data tier	IaaS, SaaS	Experience report and lessons learned	In Proceedings of the 3rd USENIX conference on Hot topics in cloud computing (pp. 5-5). USENIX Association.	87
[S19.]	Tran et al. "**Application migration to cloud: a taxonomy of critical factors**."	2011	Type IV	Not specified	PaaS	Experience report and taxonomy proposal	In Proceedings of the 2nd international workshop on software engineering for cloud computing May 22 (pp. 22-28). ACM.	51
[S20.]	Menychtas et al. **"ARTIST Methodology and Framework: A novel approach for the migration of legacy software on the Cloud."**	2013	Type V	Cloudify	SaaS	Solution proposal	In Symbolic and Numeric Algorithms for Scientific Computing (SYNASC), 2013 15th International Symposium on 2013 Sep 23 (pp. 424-431). IEEE.	15
[S21.]	Fittakau et al. **"CDOSim: Simulating Cloud Deployment Options for Software Migration Support."**	2012	Type V	Cloudify	IaaS	Solution proposal	In Maintenance and Evolution of Service-Oriented and Cloud-Based Systems (MESOCA), 2012 IEEE 6th International Workshop on the Sep 24 (pp. 37-46). IEEE.	53
[S22.]	Baserra et al. **"Cloudstep: A Step-by-Step Decision Process to Support Legacy Application Migration to the Cloud."**	2012	Not specified	Migrate the whole stack	IaaS, SaaS	Philosophical papers	In Maintenance and Evolution of Service-Oriented and Cloud-Based Systems (MESOCA), 2012 IEEE 6th International Workshop on the Sep 24 (pp. 7-16). IEEE.	51
[S23.]	Vu and Asal **"Legacy Application Migration to the Cloud: Practicability and Methodology."**	2012	Not specified	Partially migrate, data tier	PaaS, IaaS	Experience report and lessons learned	In Services (SERVICES), 2012 IEEE Eighth World Congress on Jun 24 (pp. 270-277). IEEE.	23
[S24.]	Frey et al. **"Automatic conformance checking for migrating software systems to cloud infrastructures and platforms."**	2013	Not specified	Cloudify	PaaS, IaaS	Experience report and solution proposal	Journal of Software: Evolution and Process. Oct 1;25(10):1089-115.	44
[S25.]	Ward et al. **"Workload Migration into Clouds – Challenges, Experiences, Opportunities."**	2010	Not specified	Not specified	In general,	Evaluation research	In Cloud Computing (CLOUD), 2010 IEEE 3rd International Conference on Jul 5 (pp. 164-171). IEEE.	63
[S26.]	Ma and Kauffman **"Competition between software-as-a-service vendors."**	2014	Not specified	Not specified	SaaS	Experience report	IEEE Transactions on Engineering Management. 2014 Nov;61(4):717-29.	13
[S27.]	Yu. et al. **"A Practical Architecture of Cloudification of Legacy Applications."**	2011	Type V	Cloudify	IaaS, PaaS, SaaS	Evaluation research	In Services (services), 2011 IEEE world congress on Jul 4 (pp. 17-24). IEEE.	27
[S28.]	Frey et al. **"An Extensible Architecture for Detecting Violations of a Cloud Environment's Constraints During Legacy Software System Migration."**	2011	Not specified	In general,	SaaS, IaaS, PaaS	Experience report	In Software Maintenance and Reengineering (CSMR), 2011 15th European Conference on Mar 1 (pp. 269-278). IEEE.	22
[S29.]	Mohagheghi and Saether **"Software Engineering Challenges for Migration to the Service Cloud Paradigm."**	2011	Type V	Migrate the whole stack	In general,	Experience report	In Services (SERVICES), 2011 IEEE World Congress on Jul 4 (pp. 507-514). IEEE.	63
[S30.]	Zardari and Bahsoon **"Cloud Adoption: A Goal-Oriented Requirements Engineering Approach."**	2011	Not specified	Partially migrate	In general,	Opinion papers	In ACM Proceedings of the 2nd International Workshop on Software Engineering for Cloud Computing 2011 May 22 (pp. 29-35). ACM.	63
[S31.]	Rai et al. **"Exploring the factors influencing the cloud computing adoption: a systematic study on cloud migration."**	2015	All	In general,	IaaS, PaaS, SaaS	Survey review study	SpringerPlus Journal. Dec 1;4(1):197.	10
[S32.]	Opara-Martins et al. **"Critical review of vendor lock-in and its impact on adoption of cloud computing."**	2014	Not specified	In general,	IaaS, PaaS, SaaS	Review study	In Information Society (i-Society), 2014 International Conference	18

							on Nov 10 (pp. 92-97). IEEE.	
[S33.]	Jamshidi et al. **"Cloud migration research: a systematic review."**	2013	All	In general,	IaaS, PaaS, SaaS	Systematic literature review	IEEE Transactions on Cloud Computing. Jul;1(2):142-57.	155
[S34.]	Strauch et al. "**Migrating application data to the cloud using cloud data."**	2013	All	Partially migrate	In general,	Solution proposal and evaluation research	In 3rd International Conference on Cloud Computing and Service Science, (CLOSER) (pp. 36-46).	18
[S35.]	Lewis **"Role of standards in cloud-computing interoperability."**	2012	Not specified	All	IaaS, PaaS, SaaS	Experience report and opinion papers	In System Sciences (HICSS), 2012 46th Hawaii International Conference on Jan 7 (pp. 1652-1661). IEEE.	73
[S36.]	Lloyd et al. **"Migration of Multitier Applications to Infrastructure-as-a-Service Clouds: An Investigation Using Kernel-based Virtual Machines."**	2013	Type V	Migrate whole stack	IaaS	Experience report	In Grid Computing (GRID), 2011 12th IEEE/ACM International Conference on Sep 21 (pp. 137-144). IEEE	28
[S37.]	Chauhan and Babar **"Migrating Service-Oriented System to Cloud Computing: An Experience Report"**	2011	Not specified	Cloudify	IaaS, PaaS, SaaS	Experience report	In Cloud Computing (CLOUD), 2011 IEEE International Conference on Jul 4 (pp. 404-411). IEEE.	50
[S38.]	Gholami et al. **"Cloud migration process—A survey, evaluation framework, and open challenges."**	2016	All	In general,	IaaS, PaaS, SaaS	Survey study	Journal of Systems and Software. Oct 31; 120:31-69.	6
[S39.]	Zhao and Zhou **"Strategies and methods for cloud migration."**	2014	All	In general,	IaaS, PaaS, SaaS	Opinion papers	International Journal of Automation and Computing. Apr 1;11(2):143-52.	12
[S40.]	Opara-Martins et al. **"Implications of Integration and Interoperability for Enterprise Cloud-Based Applications."**	2015	Not specified	Partially migrate	IaaS, PaaS, SaaS	Evaluation research	In Cloud Computing: 6th International Conference, CloudComp 2015, Daejeon, South Korea, October 28-29, Revised Selected Papers 2016 May 5 (Vol. 167, p. 213). Springer.	1
[S41.]	De Filippi and McCarthy "**Cloud Computing: Centralization and Data Sovereignty."**	2012	Not specified	Not specified	In general,	Validation research	European Journal of Law and Technology ;3(2).	21
[S42.]	Jansen and Grance **"Sp 800-144. Guidelines on security and privacy in public cloud computing."**	2011	Not specified	Not specified	IaaS, PaaS, SaaS	Best practice report	NIST Special Publication 800-144	744
[S43.]	Gonzalez et al**. "A quantitative analysis of current security concerns and solutions for cloud computing."**	2012	Not specified	In general,	IaaS, PaaS, SaaS	Survey study	Journal of Cloud Computing: Advances, Systems and Applications. Jul 12;1(1):11.	163
[S44.]	Yu et al. **"A practical architecture of cloudification of legacy applications."**	2011	Type IV	Cloudify	SaaS	Solution proposal	In Services (services), 2011 IEEE world congress on Jul 4 (pp. 17-24). IEEE.	27
[S45.]	Yam et al. **"Migration to Cloud as Real Option Investment decision under uncertainty."**	2011	Type II	Partially migrate	In general,	Solution proposal	In Trust, Security and Privacy in Computing and Communications (TrustCom), 2011 IEEE 10th International Conference on Nov 16 (pp. 940-949). IEEE.	19
[S46.]	Sahandi et al. **"Cloud computing from smes perspective: A survey-based investigation."**	2013	Not specified	Not specified	IaaS, PaaS, SaaS	Survey study	Journal of Information Technology Management. 2013;24(1):1-2.	35
[S47.]	Opara-Martins et al**." Critical analysis of vendor lock-in and its impact on cloud computing migration: a business perspective."**	2016	All	Partially migrate, cloudify	IaaS, PaaS, SaaS	Survey study and experience report	Journal of Cloud Computing: Advances, Systems and Applications. 2016 Dec 1;5(1):1-8.	7
[S48.]	Bergmayr et al. **"Migrating legacy software to the cloud with ARTIST."**	2013	All	Cloudify	SaaS	Solution proposal	In Software Maintenance and Reengineering (CSMR), 2013 17th European Conference on Mar 5 (pp. 465-468). IEEE.	40
[S49.]	Armbrust et al. **"A view of cloud computing."**	2010	Not specified	In general,	IaaS, PaaS, SaaS	Experience report	Communications of the ACM. 2010 Apr 1;53(4):50-8.	13065
[S50.]	Kalloniatis et al. **"Migrating into the cloud: identifying the major security and privacy concerns."**	2013	Not specified	Not specified	IaaS. PaaS, SaaS	Evaluation research	In Conference on e-Business, e-Services and e-Society 2013 Apr 25 (pp. 73-87). Springer Berlin Heidelberg.	10
[S51.]	Dillon et al. **"Cloud computing: issues**	2010	Not	Not	IaaS, PaaS,	Validation	In Advanced Information	833

	and challenges."		specified	specified	SaaS	research	Networking and Applications (AINA), 2010 24th IEEE International Conference on Apr 20 (pp. 27-33). IEEE.	
[S52.]	Janssen and Joha **"Challenges for adopting cloud-based software as a service (saas) in the public sector."**	2011	Not specified	In general,	SaaS	Evaluation research	In European Conference on Information Systems (ECIS) 2011 Jun 6.	88
[S53.]	Petcu **"Portability and interoperability between clouds: challenges and case study."**	2011	All	In general,	IaaS, PaaS, SaaS	Case study	Springer Berlin Heidelberg. In European Conference on a Service-Based Internet 2011 Oct 26 (pp. 62-74). Springer Berlin Heidelberg.	106
[S54.]	Petcu et al. **"Portable cloud applications—from theory to practice."**	2013	All	Not specified	IaaS, PaaS, SaaS	Evaluation research	Future Generation Computer Systems. 2013 Aug 31;29(6):1417-30.	142
[S55.]	Silva et al. **"A systematic review of cloud lock-in solutions."**	2013	All	In general,	IaaS, PaaS, SaaS	Systematic review study	In Cloud Computing Technology and Science (CloudCom), 2013 IEEE 5th International Conference on 2013 Dec 2 (Vol. 2, pp. 363-368). IEEE.	15
[S56.]	Ardagna et al. **"Modaclouds: A model-driven approach for the design and execution of applications on multiple clouds."**	2012	Not specified	In general,	IaaS, PaaS, SaaS	Solution proposal and evaluation study	In Proceedings of the 4th international workshop on modelling in software engineering on Jun 2 (pp. 50-56). IEEE Press.	162
[S57.]	Binz et al. **"CMotion: A Framework for Migration of Applications into and between Clouds."**	2011	Not specified	Partially migrate	In general,	Solution proposal and experience report	In Service-Oriented Computing and Applications (SOCA), 2011 IEEE International Conference on Dec 12 (pp. 1-4). IEEE.	41
[S58.]	Kurze at al. **"Cloud federation."**	2011	All	Full migration and partially migrate	IaaS, PaaS, SaaS	Philosophical papers	In Proceedings of the 2nd International Conference on Cloud Computing, GRIDs, and Virtualization (CLOUD COMPUTING 2011) Sep (Vol. 1971548541).	104
[S59.]	Zhang et al. **"A survey on cloud interoperability: taxonomies, standards, and practice."**	2013	Not specified	In general,	IaaS	Survey review study	ACM SIGMETRICS Performance Evaluation Review. Apr 29;40(4):13-22.	54
[S60.]	Laszewski and Nauduri **"Migrating to the cloud: Oracle client/server modernization."**	2011	All	In general,	IaaS, PaaS, SaaS	Book	Elsevier; 2011 Nov 8.	23
[S61.]	Jamshidi and Pahl **"Cloud Migration Patterns: A Multi-Cloud Architecture Perspective"**	2014	All	Not specified	IaaS, PaaS, SaaS	Evaluation research and opinion papers	In Service-Oriented Computing-ICSOC 2014 Workshops (pp. 6-19). Springer International Publishing.	12
[S62.]	Lindner et al. **"Understanding cloud requirements-a supply chain lifecycle approach."**	2011	Not specified	Not specified	IaaS, PaaS, SaaS	Experience reports and opinion papers	In Proceedings of the 2nd International Conference on Cloud Computing, GRIDs, and Virtualization CLOUD COMPUTING. XPS (Xpert Publishing Services).	12
[S63.]	Srivastava et al. **"A security policy oracle: Detecting security holes using multiple API implementations."**	2011	Not specified	In general,	IaaS, PaaS, SaaS	Solution proposal	ACM SIGPLAN Notices. 2011 Jun 4;46(6):343-54.	24
[S64.]	Fowley et al. **"Software System Migration to Cloud-Native Architectures for SME-Sized Software Vendors."**	2017	Not specified	In general,	SaaS, PaaS	Evaluation research	In International Conference on Current Trends in Theory and Practice of Informatics Jan 16 (pp. 498-509). Springer, Cham.	1

Assessing the Impact and Maturity of Cloud Migration Research

a. What are the fora or communities in which work on cloud migration has been published?

With respect to the publication channel where the most cloud migration research studies are published, the IEEE World Congress on Services published 5 articles, IEEE and IARIA conferences each published 3 studies as shown in **Table 6**. This table synopsises a description of the most active research communities in the field of cloud computing migration. Regarding the topics and research fora in which these studies are published, 5 were related to cloud migration decision support, 4 were related to migration execution, 6 were related to procedures and techniques for enabling legacy software migration/modernization, the other 4 studies published in Maintenance and Evolution of Service-Oriented and Cloud-based Systems group were related to general enterprise cloud migration challenges, rather than specific cloud lock-in research challenges (or questions). Finally, for the last two research groups with two publications, each were related to cloud computing migration experiments (i.e. experience reports and lessons learned) and the test (or evaluation method) involved. **Table 6** consolidates the most active research fora and communities working in the field of cloud migration research with at least two or more included studies that relates to our initial RQs. Note, these studies have been referenced earlier along with their research contribution type, cloud service model, and migration type listed in Table 3 to identify the related challenges and existing risks of vendor lock-in affecting enterprise cloud migration and adoption. In this aspect, what can be drawn from Table 6 suggests that research contributions in cloud migration and solution proposals addressing the vendor lock-in problem are published by academic and industry researchers across diverse communities and special interest groups with distinct research focus.

Overall, according to **Table 6**, the set of studies in our review are dominated by two European institution researchers who have been actively involved in several studies, the Cloud Computing Co-laboratory, School of Computer Science, University of St. Andrews have contributed 3 of the studies, followed by the Institute e-Austria Timisoara and West University of Timisoara which have been involved in 2 of the selected studies. In our review, the two researchers who contributed at least two or more cloud migration research, Khajeh-Hosseini and Petcu, are respectively affiliated with the institutions. In the selected set of studies, we also looked for the authors' affiliation details to identify active research institutes involved in work related to cloud computing migration and vendor lock-in (**Table 7**). Since writing and publishing are common tasks in research, hence it becomes critical to any researcher in a new area to identify the most relevant sources of material. To support cloud computing researchers in this direction, we show in **Table 6** and **Table 7** the journals, conferences, and institutions most targeted by researchers to publish their results and findings.

Table 6. Active Research Communities and Industry Fora focused on Cloud Computing Migration and Vendor Lock-In

Category	Study ID	Focus of Research Community/Fora
IEEE World Congress on Services	[S4] [S23] [S27] [S29] [S44]	Enable IT services and computing technology to perform business services more efficiently and effectively.
ACM Software Engineering Group for Cloud Computing	[S2] [S7] [S19] [S30]	Provide a forum for researchers, practitioners and educators to present and discuss the most recent innovations, trends, experiences and concerns in the field of software engineering and cloud computing.
IEEE Software Maintenance and Reengineering Group	[S6] [S25] [S28] [S48] [S58] [S62]	It promotes discussion and interaction among researchers and practitioners about the development of maintainable systems, and the evolution, migration and reengineering of the existing ones.
IEEE Maintenance and Evolution of Service-Oriented and Cloud-based Systems group	[S8] [S21] [S22] [S37]	Focal point and an ongoing forum for researchers and practitioners to share results and open issues in maintenance and evolution of service-oriented systems and/or cloud-based systems.
Journal of Systems and Software	[S14] [S38]	Publishes articles covering all aspects of cloud software engineering and related hardware-software-systems issues.
Journal of Cloud Computing: Advances, Systems and Applications	[S43] [S47]	Principally publish research articles on all aspects of cloud computing, addressing topics that are core to cloud computing, focusing on the cloud applications, the cloud systems, and the advances that will lead to the clouds of the future

Table 7 Most Active Research Institutions

Institution Name	Study ID	Number of Studies
Irish Centre for Cloud Computing and Commerce (IC4), Dublin City University, Ireland	[S1, S33, S61, S64]	4
University of Kiel, Germany	[S6, S21, S24, S28]	4
Bournemouth University, United Kingdom (UK)	[S32, S40, S47, S32]	4
Institute of Architecture of Application Systems (IAAS), University of Stuttgart, Germany	[S3, S34, S57]	3

- **Distribution by Author's Institution**

Table 8 represents the geographical distribution of the identified papers. As shown in the table below, the sample distribution across the continents and country of author's institutions was recorded in terms of both percent distribution and absolute numbers since the sample size drives the ability to find the statistical significance. For instance, the publication count (i.e. Pc) in the table indicates the total number of times author(s) from a country published a paper on the topic of cloud (SaaS) migration and vendor lock-in. However, please note that for collaborative research papers, with one or more authors from different nationality, the country of the first authors' institution is referenced in **Table 8**.

Table 8 Distribution of Studies by Author's Nationality

Continent	Country of Institution	Publication Count (Pc)	Percentage Value (Pv)
North and South America	USA	11	17.1%
	Brazil	2	3.1%
	Canada	1	1.6%
	Total	**14**	**~22%**
Europe	Germany	10	15.63%
	United Kingdom (UK)	9	14.1%
	Ireland	3	4.7%
	Greece	2	3.1%
	Norway	2	3.1%
	Romania	2	3.1%
	Denmark	1	1.6%
	Sweden	1	1.6%
	France	1	1.6%
	Austria	1	1.6%
	Netherlands	1	1.6%
	Italy	1	1.6%
	Total	**34**	**~53.13%**
Asia Pacific	China	3	4.7%
	Hong Kong	2	3.13%
	India	2	3.13%
	Singapore	1	1.6%
	United Arab Emirates (UAE)	1	1.6%
	Total	**9**	**~14.1%**
Australia	Australia	7	11%
	Total	**7**	**~11%**

Organising the publication count based on the continent has been listed in descending order of preference to show the percentage value of countries with the highest to smallest number of papers. As shown in this table, institutions in the USA ranked first with more (11) publication counts (17.1%) in the field of cloud computing migration compared to other countries. Germany stands at second place with 10 publication counts (15.63%), followed by United Kingdom (UK) at third place with 9 publication counts (14.1%), and Australia at fourth place with 7 papers (11% of total publication count). However, Ireland (4.7%) and China (4.7%) both published 3 papers each, while Romania, Greece, Hong Kong, India, and Brazil all published 2 papers respectively. Finally, Sweden, France, Austria, Canada, Singapore, United Arab Emirates and the Netherlands all with 1 published paper respectively.

In terms of future research directions in this aspect, it would be encouraging to see contributions from research institutes located in Africa since our review study has shown null papers in this region. In looking at attitudes and expectations for cloud computing in Africa, the findings of this review are consistent with IDG survey of organisations in Algeria, Kenya, Morocco, Nigeria and South Africa. Most organizations in those countries

"have either already moved some virtual workloads, applications or services into cloud hosted infrastructure, platform or software-as-a-service environments, or are preparing to do so, yet a sizable minority have yet to engage in cloud migration strategy on any meaningful scale (IDG, 2015). Whilst this suggests a relative immaturity of the wider African market for cloud services compared to Europe, it also highlights the scope of the commercial opportunity for cloud service providers in the region looking for potential customers." This observation is quite insightful considering that the African continent is set for significant cloud adoption, according to this study from SAP and IDG, with some concerns and potential advantages unique to the region.

Bibliography

- Weinhardt C, Anandasivam A, Blau B, Borissov N, Meinl T, Michalk W, Stößer J. Cloud computing–a classification, business models, and research directions. Business & Information Systems Engineering. 2009 Oct 1;1(5):391-9.
- Creeger, M. (2009). CTO roundtable. Communications of the ACM, 52, 50.
- Cusumano, M. (2010). Cloud computing and SaaS as new computing platforms. Communications of the ACM, 53, 27–29.
- Garrison, G., Kim, S., & Wakefield, R. L. (2012). Success factors for deploying cloud computing. Communications of the ACM, 55, 62. Hayes, B. (2008). Cloud computing. Communications of the ACM, 51, 9–11.
- Hoberg, P., Wollersheim, J., & Krcmar, H. (2012). The business perspective on Cloud Computing: A literature review of research on Cloud Computing. In Proceedings of the AMCIS.
- Iyer, B., & Henderson, J. C. (2010). Preparing for the future— understanding the seven capabilities of Cloud Computing. MIS Quarterly Executive (pp. 117–131).
- Kaisler, S., Money, W. H., & Cohen, S. J. (2012). A decision framework for Cloud Computing. In Proceedings of the HICSS (pp. 1553–1562). IEEE
- F. Gonidis, A. J. H. Simons, I. Paraskakis, and K. Dimitrios, "Cloud application portability: an initial view," p. 275, 2013.
- Keele, S. Guidelines for performing systematic literature reviews in software engineering. In Technical report, Ver 2.3 EBSE Technical Report. EBSE. Sn.
- Chauhan, M.A., Babar, M.A.: Towards process support for migrating applications to cloud computing. In: 2012 International Conference on Cloud and Service Computing. pp. 80–87. IEEE Computer Society (2012)
- Beserra, P.V., Camara, A., Ximenes, R., Albuquerque, A.B., Mendonca, N.C.: Cloudstep: A step-by-step decision process to support legacy application migration to the cloud. In: Maintenance and Evolution of Service-Oriented and Cloud-Based Systems (MESOCA 2012) Workshop. pp. 7–16. IEEE (2012)
- Hajjat, M., Sun, X., Sung, Y., Maltz, D., Rao, S., Sripanidkulchai, K., Tawarmalani, M.: Cloudward bound: planning for beneficial migration of enterprise applications to the cloud. In: ACM SIGCOMM Computer Communication Review. vol. 40, pp. 243–254. ACM (2010)
- Khajeh-Hosseini, A., Greenwood, D., Smith, J.W., Sommerville, I.: The cloud adoption toolkit: supporting cloud adoption decisions in the enterprise. Software: Practice and Experience 42(4), 447–465 (2012)
- Jamshidi, P., Ahmad, A., Pahl, C.: Cloud Migration Research: A Systematic Review. IEEE Transactions on Cloud Computing 1(2) (2013)
- Pardo, J., Flavin, A. and Rose, M. (2016). 2016 Top Markets Report - Cloud Computig [Online]. Available from: http://www.trade.gov/topmarkets/pdf/Cloud_Computing_United_Kingdom.pdf Accessed on 7th November 2016.
- King, I. (2014) Cloud Spending by Companies Outpaces Predictions, Forrester Says [Online]. Available from: https://www.bloomberg.com/news/articles/2014-04-24/cloud-spending-by-companies-outpaces-predictions-forrester-says Accessed on 7th November 2016
- Casemore, B., (2014) The Rise of the Hybrid WAN: Meeting the Challenge of the Cloud [Online]. Available from: https://www.silver-peak.com/sites/default/files/infoctr/idc_wp_rise-of-the-hybrid-wan.pdf Accessed 8th November 2016

- Cisco, (2015) Cisco Global Cloud Index: Forecast and Methodology [Online]. Available from: http://www.cisco.com/c/dam/en/us/solutions/collateral/service-provider/global-cloud-index-gci/white-paper-c11-738085.pdf Accessed 12th November 2016
- Guzzo, R.A., S.E. Jackson, and R.A. Katzell (1987) "Meta-analysis Analysis," Research in Organizational Behavior (9), pp. 407–442
- Columbus, L. (2014) IDC Predicts SaaS Enterprise Applications Will Be a $50.8B Market by 2018 [Online]. Available from: https://www.forbes.com/sites/louiscolumbus/2014/12/20/idc-predicts-saas-enterprise-applications-will-be-a-50-8b-market-by-2018/#3bc93dcc22a8 Accessed 12th November 2016
- Petticrew, Mark and Helen Roberts. Systematic Reviews in the Social Sciences: A Practical Guide, Blackwell Publishing, 2005, ISBN 1405121106
- Gartner, (2016) Hybrid Will Be the Most Common Use of the Cloud [Online]. Available from: http://www.gartner.com/newsroom/id/3354117 Accessed 14th November 2016
- Rai, R., Sahoo, G. and Mehfuz, S., 2015. Exploring the factors influencing the cloud computing adoption: a systematic study on cloud migration. *SpringerPlus*, *4*(1), p.197.
- IDC, (2010) "Cloud computing 2010 – an IDC update," [Online]. Available from: http://www.cionet.com/Data/files/groups/Cloud%20Computing%20201 0%20-%20An%20IDC%20Update.pdf [Online] Accessed on 12th January 2016.
- Cloud Industry Forum (CIF), (2015) "Making sense of Hybrid IT: Cloud computing now the norm in a predominantly Hybrid IT Market," 2015 [Online] Available from: http://cloudindustryforum.org/news/582-cloudcomputing-now-the-norm-in-a-predominantly-hybrid-it-market Accessed on 11 February 2016
- Hwang, K., and D. Li (2010) "Trusted Cloud Computing with Secure Resources and Data Colouring," IEEE Internet Computing (14)5, p. 14.
- Hwang, M.I., and R.G. Thorn (1999) "The Effect of User Engagement on System Success: A Meta-Analytical Integration of Research Findings," Information & Management (35), pp. 229–236.
- Marston, S., Li, Z., Bandyopadhyay, S., Zhang, J. and Ghalsasi, A., (2011). Cloud computing—the business perspective. Decision support systems, 51(1), pp.176-189.
- Petter, S., and E.R. McLean (2009) "A Meta-Analytic Assessment of the Delone and Mclean IS Success Model: An Examination of IS Success at the Individual Level," Information & Management (46)3, pp. 159–166.
- M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. H. Katz, A. Konwinski, G. Lee, D. A. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, "Above the clouds: A berkeley view of cloud
- Computing," Feb 2009.
- Sabherwal, R., A. Jeyaraj, and C. Chowa (2006) "Information System Success: Individual and Organizational Determinants," Management Science (52)12, p. 1849.
- L. Schubert, K. Jeffery, and B. Neidecker-Lutz, "The future of cloud computing," European Commission - Information Society and Media, Tech. Rep., 2010.
- Yang, H. and Tate, M., 2012. A descriptive literature review and classification of cloud computing research. *Communications of the Association for Information Systems*, *31*(2), pp.35-60.
- A. Khajeh-Hosseini, I. Sommerville, and I. Sriram, "Research challenges for enterprise cloud computing," Information Security, no. 1960, 2010.
- Kitchenham, B., 2004. In: Procedures for Undertaking Systematic Reviews. Joint Technical Report, Computer Science Department, Keele University (TR/SE-0401) and National ICT Australia Ltd (0400011T.1).
- Robey, D. and Markus, M.L. (1997), "Beyond Rigor and Relevance: Producing Consumable Research About Information Systems", Information Resources Management Journal
- D. Catteddu and G. Hogben, "Cloud computing - benefits, risks and recommendations for information security," European Network and Information Security Agency, Tech. Rep., 2009.
- Weinhardt, C., Anandasivam, A., Blau, B., Borissov, N., Meinl, T., Michalk, W. and Stößer, J., 2009. Cloud computing–a classification, business models, and research directions. *Business & Information Systems Engineering*, *1*(5), pp.391-399.

- V. Nelson and V. Uma, "Semantic based Resource Provisioning and scheduling in inter-cloud environment," in International Conference on Recent Trends in Information Technology, 2012, pp. 250–254.
- Pahl, C., Xiong, H. and Walshe, R., 2013, September. A comparison of on-premise to cloud migration approaches. In *European Conference on Service-Oriented and Cloud Computing* (pp. 212-226). Springer Berlin Heidelberg.
- L. Rodero-Merino, L. M. Vaquero, V. Gil, F. Galán, J. Fontán, R. S. Montero, and I. M. Llorente, "From infrastructure delivery to service management in clouds," Future Generation Computer Systems, vol. 26, no. 8, pp. 1226–1240, Oct. 2010.
- Babar, M.A. and Chauhan, M.A., 2011, May. A tale of migration to cloud computing for sharing experiences and observations. In *Proceedings of the 2nd international workshop on software engineering for cloud computing* (pp. 50-56). ACM.
- A. Sampaio and N. Mendonça, "Uni4Cloud," in 2nd Intl. workshop on Software engineering for cloud computing, 2011, pp. 15–21
- Andrikopoulos, V., Binz, T., Leymann, F. and Strauch, S., 2013. How to adapt applications for the cloud environment. *Computing*, *95*(6), pp.493-535.
- J. Tao, H. Marten, D. Kramer, and W. Karl, "An Intuitive Framework for Accessing Computing Clouds," Procedia Computer Science, vol. 4, no. 1, pp. 2049–2057, Jan. 2011.
- Mohagheghi, P. and Sæther, T., 2011, July. Software engineering challenges for migration to the service cloud paradigm: Ongoing work in the remics project. In *Services (SERVICES), 2011 IEEE World Congress on* (pp. 507-514). IEEE.
- H. Abu-Libdeh, L. Princehouse, and H. Weatherspoon, "RACS: a case for cloud storage diversity," in 1st ACM SoCC '10, 2010, pp. 229–240.
- Buyya, R., Ranjan, R. and Calheiros, R., 2010. Intercloud: Utility-oriented federation of cloud computing environments for scaling of application services. *Algorithms and architectures for parallel processing*, pp.13-31.
- N. Loutas, V. Peristeras, T. Bouras, E. Kamateri, D. Zeginis, and K. Tarabanis, "Towards a Reference Architecture for Semantically Interoperable Clouds," in 2010 IEEE Second International Conference on Cloud Computing Technology and Science, 2010, pp. 143–150.
- King, W.R., and J. He (2005) "Understanding the Role and Methods of Meta-Analysis in IS Research," Communications of the Association for Information Systems (16) Article 32, pp. 665-686.
- B. Rochwerger, D. Breitgand, E. Levy, A. Galis, K. Nagin, I. M. Llorente, R. S. Montero, Y. Wolfsthal, E. Elmroth, J. Caceres, M. BenYehuda, W. Emmerich, and F. Galán, "The Reservoir model and architecture for open federated cloud computing," IBM Journal of Research and Development, vol. 53, no. 4, pp. 4:1–4:11, Jul. 2009.
- Frey, S. and Hasselbring, W., 2010. Model-based migration of legacy software systems to scalable and resource-efficient cloud-based applications: The cloudmig approach.
- P. Hofmann and D. Woods, "Cloud Computing: The Limits of Public Clouds for Business Applications," IEEE Internet Computing, vol. 14, no. 6, pp. 90–93, Nov. 2010.
- Tran, V., Keung, J., Liu, A. and Fekete, A., 2011, May. Application migration to cloud: a taxonomy of critical factors. In *Proceedings of the 2nd international workshop on software engineering for cloud computing* (pp. 22-28). ACM.
- Liu X, Ye H (2008) A Sustainable Service-Oriented B2C Framework for Small Businesses. In 4th IEEE International Symposium on Service Oriented Systems Engineering (SOSE'08), Taiwan, December.
- Khajeh-Hosseini, A., Greenwood, D. and Sommerville, I., 2010, July. Cloud migration: A case study of migrating an enterprise it system to iaas. In *Cloud Computing (CLOUD), 2010 IEEE 3rd International Conference on* (pp. 450-457). IEEE.
- Petcu D (2011) Portability and Interoperability between Clouds: Challenges and Case Study. In: Towards a Service-Based Internet, vol 6994. Springer, Berlin Heidelberg, pp 62–74
- Srinivasan, M.K., Sarukesi, K., Rodrigues, P., Manoj, M.S. and Revathy, P., 2012, August. State-of-the-art cloud computing security taxonomies: a classification of security challenges in the present cloud

computing environment. In *Proceedings of the international conference on advances in computing, communications and informatics* (pp. 470-476). ACM.

- Miranda J, Guillen J, Murillo J (2012) Identifying Adaptation Needs to Avoid the Vendor Lock-in Effect in the Deployment of Cloud ServiceBased Applications (SBAs). WAS4FI I-Mashups September 19 Bertinoro, Italy.
- Hajjat, M., Sun, X., Sung, Y.W.E., Maltz, D., Rao, S., Sripanidkulchai, K. and Tawarmalani, M., 2010, August. Cloudward bound: planning for beneficial migration of enterprise applications to the cloud. In *ACM SIGCOMM Computer Communication Review* (Vol. 40, No. 4, pp. 243-254). ACM.
- D. Nurmi, R. Wolski, C. Grzegorczyk, G. Obertelli, S. Soman, L. Youseff, and D. Zagorodnov, "The Eucalyptus Open-Source Cloud-Computing System," Proc. of IEEE International Symposium on Cluster Computing and the Grid (CCGrid), 2009
- Zhang, Q., Cheng, L. and Boutaba, R., 2010. Cloud computing: state-of-the-art and research challenges. *Journal of internet services and applications*, *1*(1), pp.7-18.
- Taylor, R.C., 2010. An overview of the Hadoop/MapReduce/HBase framework and its current applications in bioinformatics. BMC bioinformatics, 11(12), p.S1. Vancouver
- Webster, J., and R.T. Watson (2002) "Analysing the Past to Prepare for the Future: Writing a Literature Review," MIS Quarterly (26)2, pp. iii–xiii.
- Khajeh-Hosseini, A., Sommerville, I. and Sriram, I., 2010. Research challenges for enterprise cloud computing. *arXiv preprint arXiv:1001.3257*.
- Menzel, M. and Ranjan, R., 2012, April. CloudGenius: decision support for web server cloud migration. In *Proceedings of the 21st international conference on World Wide Web* (pp. 979-988). ACM.
- Gholami, M.F., Daneshgar, F., Low, G. and Beydoun, G., 2016. Cloud migration process—A survey, evaluation framework, and open challenges. *Journal of Systems and Software*, *120*, pp.31-69.
- Alhamad, M., Dillon, T. and Chang, E., 2010, April. Conceptual SLA framework for cloud computing. In *Digital Ecosystems and Technologies (DEST), 2010 4th IEEE International Conference on* (pp. 606-610). IEEE.
- Zhu, K.X. and Zhou, Z.Z., 2012. Research note—Lock-in strategy in software competition: Open-source software vs. proprietary software. *Information Systems Research*, *23*(2), pp.536-545.
- Khajeh- Hosseini, A., Greenwood, D., Smith, J.W. and Sommerville, I., 2012. The cloud adoption toolkit: supporting cloud adoption decisions in the enterprise. *Software: Practice and Experience*, *42*(4), pp.447-465.
- Tak, B.C., Urgaonkar, B. and Sivasubramaniam, A., 2011, June. To Move or Not to Move: The Economics of Cloud Computing. In *HotCloud*.
- Tran, V., Keung, J., Liu, A. and Fekete, A., 2011, May. Application migration to cloud: a taxonomy of critical factors. In *Proceedings of the 2nd international workshop on software engineering for cloud computing* (pp. 22-28). ACM.
- Menychtas, A., Santzaridou, C., Kousiouris, G., Varvarigou, T., Orue-Echevarria, L., Alonso, J., Gorronogoitia, J., Bruneliere, H., Strauss, O., Senkova, T. and Pellens, B., 2013, September. ARTIST Methodology and Framework: A novel approach for the migration of legacy software on the Cloud. In *Symbolic and Numeric Algorithms for Scientific Computing (SYNASC), 2013 15th International Symposium on* (pp. 424-431). IEEE.
- Fittkau, F., Frey, S. and Hasselbring, W., 2012, September. CDOSim: Simulating cloud deployment options for software migration support. In *Maintenance and Evolution of Service-Oriented and Cloud-Based Systems (MESOCA), 2012 IEEE 6th International Workshop on the* (pp. 37-46). IEEE.
- Beserra, P.V., Camara, A., Ximenes, R., Albuquerque, A.B. and Mendonça, N.C., 2012, September. Cloudstep: A step-by-step decision process to support legacy application migration to the cloud. In *Maintenance and Evolution of Service-Oriented and Cloud-Based Systems (MESOCA), 2012 IEEE 6th International Workshop on the* (pp. 7-16). IEEE.
- Vu, Q.H. and Asal, R., 2012, June. Legacy application migration to the cloud: Practicability and methodology. In *Services (SERVICES), 2012 IEEE Eighth World Congress on* (pp. 270-277). IEEE.
- Frey, S., Hasselbring, W. and Schnoor, B., 2013. Automatic conformance checking for migrating software systems to cloud infrastructures and platforms. *Journal of Software: Evolution and Process*, *25*(10), pp.1089-1115.

- Ward, C., Aravamudan, N., Bhattacharya, K., Cheng, K., Filepp, R., Kearney, R., Peterson, B., Shwartz, L. and Young, C.C., 2010, July. Workload migration into clouds challenges, experiences, opportunities. In *Cloud Computing (CLOUD), 2010 IEEE 3rd International Conference on* (pp. 164-171). IEEE.
- Ma, D. and Kauffman, R.J., 2014. Competition between software-as-a-service vendors. *IEEE Transactions on Engineering Management*, *61*(4), pp.717-729.
- Yu, D., Wang, J., Hu, B., Liu, J., Zhang, X., He, K. and Zhang, L.J., 2011, July. A practical architecture of cloudification of legacy applications. In *Services (services), 2011 IEEE world congress on* (pp. 17-24). IEEE.
- Frey, S. and Hasselbring, W., 2011, March. An extensible architecture for detecting violations of a cloud environment's constraints during legacy software system migration. In *Software Maintenance and Reengineering (CSMR), 2011 15th European Conference on* (pp. 269-278). IEEE.
- Mohagheghi, P. and Sæther, T., 2011, July. Software engineering challenges for migration to the service cloud paradigm: Ongoing work in the remics project. In *Services (SERVICES), 2011 IEEE World Congress on* (pp. 507-514). IEEE.
- Zardari, S. and Bahsoon, R., 2011, May. Cloud adoption: a goal-oriented requirements engineering approach. In *Proceedings of the 2nd International Workshop on Software Engineering for Cloud Computing* (pp. 29-35). ACM.
- Rai, R., Sahoo, G. and Mehfuz, S., 2015. Exploring the factors influencing the cloud computing adoption: a systematic study on cloud migration. *SpringerPlus*, *4*(1), p.197.
- Opara-Martins, J., Sahandi, R. and Tian, F., 2014, November. Critical review of vendor lock-in and its impact on adoption of cloud computing. In *Information Society (i-Society), 2014 International Conference on* (pp. 92-97). IEEE.
- Jamshidi, P., Ahmad, A. and Pahl, C., 2013. Cloud migration research: a systematic review. *IEEE Transactions on Cloud Computing*, *1*(2), pp.142-157.
- Strauch, S., Andrikopoulos, V. and Bachmann, T., 2013. Migrating application data to the cloud using cloud data. In *e 3rd International Conference on Cloud Computing and Service Science, (CLOSER)* (pp. 36-46).
- Lewis, G.A., 2013, January. Role of standards in cloud-computing interoperability. In *System Sciences (HICSS), 2013 46th Hawaii International Conference on* (pp. 1652-1661). IEEE.
- Lloyd, W., Pallickara, S., David, O., Lyon, J., Arabi, M. and Rojas, K., 2011, September. Migration of multi-tier applications to infrastructure-as-a-service clouds: An investigation using kernel-based virtual machines. In *Grid Computing (GRID), 2011 12th IEEE/ACM International Conference on* (pp. 137-144). IEEE.
- Chauhan, M.A. and Babar, M.A., 2011, July. Migrating service-oriented system to cloud computing: An experience report. In *Cloud Computing (CLOUD), 2011 IEEE International Conference on* (pp. 404-411). IEEE.
- Gholami, M.F., Daneshgar, F., Low, G. and Beydoun, G., 2016. Cloud migration process—A survey, evaluation framework, and open challenges. *Journal of Systems and Software*, *120*, pp.31-69.
- Zhao, J.F. and Zhou, J.T., 2014. Strategies and methods for cloud migration. *International Journal of Automation and Computing*, *11*(2), pp.143-152.
- Opara-Martins, J., Sahandi, R. and Tian, F., 2015, October. Implications of integration and interoperability for enterprise cloud-based applications. In *International Conference on Cloud Computing* (pp. 213-223). Springer International Publishing.
- De Filippi, P. and McCarthy, S., 2012. Cloud Computing: Centralization and Data Sovereignty.
- Jansen, W. and Grance, T., 2011. Sp 800-144. Guidelines on security and privacy in public cloud computing.
- Gonzalez, N., Miers, C., Redigolo, F., Simplicio, M., Carvalho, T., Näslund, M. and Pourzandi, M., 2012. A quantitative analysis of current security concerns and solutions for cloud computing. *Journal of Cloud Computing: Advances, Systems and Applications*, *1*(1), p.11.
- Yu, D., Wang, J., Hu, B., Liu, J., Zhang, X., He, K. and Zhang, L.J., 2011, July. A practical architecture of cloudification of legacy applications. In *Services (services), 2011 ieee world congress on* (pp. 17-24). IEEE.
- Yam, C.Y., Baldwin, A., Shiu, S. and Ioannidis, C., 2011, November. Migration to cloud as real option: Investment decision under uncertainty. In *Trust, Security and Privacy in Computing and Communications (TrustCom), 2011 IEEE 10th International Conference on* (pp. 940-949). IEEE.

- Sahandi, R., Alkhalil, A. and Opara-Martins, J., 2013. Cloud computing from smes perspective: A survey-based investigation. *Journal of Information Technology Management*, *24*(1), pp.1-12.
- Opara-Martins, J., Sahandi, R. and 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), pp.1-18.
- Bergmayr, A., Bruneliere, H., Izquierdo, J.L.C., Gorronogoitia, J., Kousiouris, G., Kyriazis, D., Langer, P., Menychtas, A., Orue-Echevarria, L., Pezuela, C. and Wimmer, M., 2013, March. Migrating legacy software to the cloud with ARTIST. In *Software Maintenance and Reengineering (CSMR), 2013 17th European Conference on* (pp. 465-468). IEEE.
- Armbrust, M., Fox, A., Griffith, R., Joseph, A.D., Katz, R., Konwinski, A., Lee, G., Patterson, D., Rabkin, A., Stoica, I. and Zaharia, M., 2010. A view of cloud computing. *Communications of the ACM*, *53*(4), pp.50-58.
- Kalloniatis, C., Manousakis, V., Mouratidis, H. and Gritzalis, S., 2013, April. Migrating into the cloud: identifying the major security and privacy concerns. In *Conference on e-Business, e-Services and e-Society* (pp. 73-87). Springer Berlin Heidelberg.
- Dillon, T., Wu, C. and Chang, E., 2010, April. Cloud computing: issues and challenges. In *Advanced Information Networking and Applications (AINA), 2010 24th IEEE International Conference on* (pp. 27-33). IEEE.
- Janssen, M. and Joha, A., 2011, June. Challenges for adopting cloud-based software as a service (saas) in the public sector. In *ECIS*.
- Petcu, D., 2011, October. Portability and interoperability between clouds: challenges and case study. In *European Conference on a Service-Based Internet* (pp. 62-74). Springer Berlin Heidelberg.
- Petcu, D., Macariu, G., Panica, S. and Crăciun, C., 2013. Portable cloud applications—from theory to practice. *Future Generation Computer Systems*, *29*(6), pp.1417-1430.
- Silva, G.C., Rose, L.M. and Calinescu, R., 2013, December. A systematic review of cloud lock-in solutions. In *Cloud Computing Technology and Science (CloudCom), 2013 IEEE 5th International Conference on* (Vol. 2, pp. 363-368). IEEE.
- Ardagna, D., Di Nitto, E., Casale, G., Petcu, D., Mohagheghi, P., Mosser, S., Matthews, P., Gericke, A., Ballagny, C., D'Andria, F. and Nechifor, C.S., 2012, June. Modaclouds: A model-driven approach for the design and execution of applications on multiple clouds. In *Proceedings of the 4th international workshop on modeling in software engineering* (pp. 50-56). IEEE Press.
- Binz, T., Leymann, F. and Schumm, D., 2011, December. CMotion: A Framework for Migration of Applications into and between Clouds. In *Service-Oriented Computing and Applications (SOCA), 2011 IEEE International Conference on* (pp. 1-4). IEEE.
- Kurze, T., Klems, M., Bermbach, D., Lenk, A., Tai, S. and Kunze, M., 2011, September. Cloud federation. In *Proceedings of the 2nd International Conference on Cloud Computing, GRIDs, and Virtualization (CLOUD COMPUTING 2011)* (Vol. 1971548541).
- Zhang, Z., Wu, C. and Cheung, D.W., 2013. A survey on cloud interoperability: taxonomies, standards, and practice. *ACM SIGMETRICS Performance Evaluation Review*, *40*(4), pp.13-22.
- Laszewski, T. and Nauduri, P., 2011. *Migrating to the cloud: Oracle client/server modernization*. Elsevier.
- Jamshidi, P., Pahl, C., Chinenyeze, S. and Liu, X., 2015. Cloud migration patterns: a multi-cloud service architecture perspective. In *Service-Oriented Computing-ICSOC 2014 Workshops* (pp. 6-19). Springer International Publishing.
- Lindner, M., McDonald, F., Conway, G. and Curry, E., 2011. Understanding cloud requirements-a supply chain lifecycle approach. In *Proceedings of the Second International Conference on Cloud Computing, GRIDs, and Virtualization CLOUD COMPUTING 2011*. XPS (Xpert Publishing Services).
- Srivastava, V., Bond, M.D., McKinley, K.S. and Shmatikov, V., 2011. A security policy oracle: Detecting security holes using multiple API implementations. *ACM SIGPLAN Notices*, *46*(6), pp.343-354.
- Fowley, F., Elango, D.M., Magar, H. and Pahl, C., 2017, January. Software System Migration to Cloud-Native Architectures for SME-Sized Software Vendors. In *International Conference on Current Trends in Theory and Practice of Informatics* (pp. 498-509). Springer, Cham.

APPENDIX 2

Research Methodology Framework

INTERVIEW

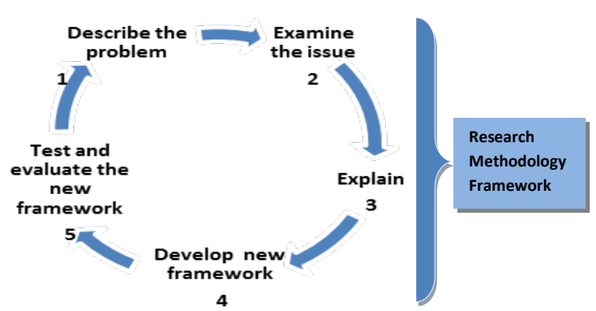
1. Has your company implemented OR is it currently using any cloud computing services?
2. What **advantages** does cloud computing bring to your company?
3. Currently, what are the main **barriers** for adoption of cloud computing in your company?
4. From your organizations perspective, what factors are key to cloud **adoption** and why?
5. What approach to cloud computing is your company taking (or likely to take) and what impels such decision?
6. Cloud computing delivers SaaS, PaaS, and IaaS services, which do you consider relevant to your company and why?
7. Which cloud computing provider(s) are you using and why?
8. Did your company negotiate the **cloud service agreement** rather than accepting the cloud provider's standard contract?
9. What **business process** has been migrated OR is your company willing to **migrate** into cloud?
10. Did your company make any **changes** to its organization structure, processes and culture in adopting cloud technology?
11. What **risks** has your company identified in moving to the cloud and how does it plan to mitigate those risks?
12. How is your company able to create and manage all legal contracts accordingly?
13. Could you please comment on the **security** aspect of cloud computing?
14. What is your view on the issue of **vendor lock-in** in the context of cloud computing?
15. In your opinion, what are the main **risks** associated with **vendor lock-in** that could potentially deter companies from adopting cloud computing services?
16. Beyond those risks identified above, could there be some tangible benefits associated with vendor lock-in?
17. If, perhaps in the future you decide to change cloud providers, how easy do you think your company can move its data to another provider or back in-house?
18. How does your company evaluate the risk of vendor lock-in?
19. What are your **concerns** for being locked-in to a single cloud provider?
20. What do you think the **main impact** of vendor lock-in will be on adoption of cloud computing?
21. How do you think companies can be **proactive/reactive** in addressing vendor lock-in risks in cloud computing?
22. Are there other issues experienced during and after migration we didn't talk about that you wish we had?

OBJECTIVES

1. Review and analyse the current usage and adoption level of cloud computing by enterprise organizations.
2. Explore views of professional practitioners on issues associated with **vendor lock-in.**
3. Identify, analyse and explore the technical, legal, and business issues associated with **vendor lock-in**.
   - 3.1 What are the security, technical (and or technological) risks associated with **vendor lock-in** problem in cloud computing?
   - 3.2 What are the legal challenges and associated **risks of vendor lock**-in in cloud computing?
4. Review cloud providers' standard contract terms of services and Service Level Agreements (SLAs) as an attempt to find a general pattern in addressing or exploiting the **lock-in** problem.
   - 4.1 Identify business-related issues with cloud contract **lock-in** and review their implications on adoption of cloud computing.
5. Identify policy and industry recommendations that could potentially steer the development of a **vendor-neutral** cloud marketplace.
   - 5.1 Identify standards that support **interoperability** between different cloud providers network
   - 5.2 Identify standards that facilitate the **portability** of data from one vendor to another.
6. Create a list of **strategic guidelin**es to follow in creating a **Cloud-based Risk Management framework** to mitigate the **risks of vendor lock-in**.
7. Propose a framework that minimises **vendor lock-in** problem in cloud computing.
8. Test and evaluate the proposed framework.

LITERATURE REVIEW

CONTRIBUTION TO KNOWLEDGE



Key: reps Interview; reps. Questionnaire; reps Objectives; reps Lit. Review and; reps. Contribution to knowledge. NB the relationship between each component is represented using an arrow.

QUESTIONNAIRE

1. Which of the following best describes the **adoption** of cloud computing in your organization?
2. The reasons behind using Cloud Computing services in your organization are?
3. What does your organization view as the **most important** benefits of using Cloud Computing technology and/or services?
4. What are the greatest **barriers** for implementing cloud computing in your organization?
5. Are you considering moving **business critical systems** (or applications) to the cloud?
6. How important is it for your organization to **integrate existing** (on-premise) IT asset with cloud-based services?
7. How would you express your current understanding of the term **Vendor Lock-In** (in cloud computing context)?
8. Do **Vendor Lock-In** risks deter your organization from adopting cloud services?
9. Please identify which **interoperability** or **data portability** issues you have encountered when using cloud services.
10. From your perspective, which existing or emerging **standards** support Interoperability across clouds and Portability of data?
11. To the best of your knowledge, how can the risks of **Vendor Lock-in** be minimised in cloud computing environment?
12. Which of these types of cloud computing is your organization currently using?
13. Which of the following cloud types has your organization adopted?
14. How concerned, if at all, are you about the security of your organization data in cloud storage?
15. Did your organization negotiate a cloud **service agreement** rather than accepting the cloud provider's standard contract/SLA agreement?
16. When negotiating with a cloud service provider, which of the following agreements should be included in the contract/SLA?
17. Does the SLA/contract specify an exit strategy upon contract termination?
18. Which one of the following applications are currently using cloud services in your organization?
19. How severe may your business operation and processes be affected by any of the vendor lock-in risks and disruptions?
20. How likely do you consider using a cloud-based **Vendor Risk Management** solution if such a framework allowed your business to understand and manage vendor lock-in risks and compliance requirements effectively?
21. What skills should be in place for proper cloud computing services implementation?
22. To what extent does geographical location matter in regard to where your organization data is stored?

APPENDIX 3

Pilot Interview Consent Form

Title of project: Decision Framework to Avoid Vendor Lock-in Risks in Cloud (SaaS) Migration

Name, position and contact details of researcher:
Mr Justice Opara-Martins FHEA (AMBCS)
Doctoral Academic Researcher in Cloud Computing
P 517B, Poole House,
Faculty of Sciences and Technology,
Bournemouth University,
Fern Barrow, Poole
Dorset, BH12 5BB. UK
Telephone: 01202961326; Email: joparamartins@bournemouth.ac.uk

Please Initial Here

I confirm that I have read and understood the participant information sheet for the above research project and have had the opportunity to ask questions.	
I understand that my participation is voluntary and that I am free to withdraw at any time, without giving reason and without there being any negative consequences. In addition, should I not wish to answer any specific question(s), complete a test or give a sample, I am free to decline.	
I give permission for members of the research team to have access to my anonymised responses. I understand that my name will not be linked with the research materials, and I will not be identified or identifiable in the report or reports that result from the research. OR *(only use one of these statements and delete the other)* I give permission for members of the research team to use my identifiable information for the purposes of this research project.	
I agree to take part in the above research project.	

_____ _____ _____

Name of Participant Date Signature

_____ _____ _____

Name of Researcher Date Signature

Once this has been signed by all parties the participant should receive a copy of the signed and dated participant consent form, the participant information sheet and any other written information provided to the participants. A copy of the signed and dated consent form should be kept with the project's main documents which must be kept in a secure location.

APPENDIX 4

Analysis of Variance (One-Way ANOVA) Test Results for Framework Evaluation

Understanding How Vendor Lock-In Impacts on Adoption of Cloud Computing

About this Questionnaire

Dear Sir / Madam

Thank you for participating in this survey. This study is concerned with investigating the current usage and adoption level of cloud computing by large corporations or small to medium-sized enterprises (SMEs). More specifically, the research aims to investigate the business related risks of vendor lock-in affecting cloud adoption and implementation by organisations. The focus of this questionnaire is to identify and evaluate the risks and opportunities which affect stakeholders' decision-making about adopting cloud services. The questionnaire compromises of 28 short questions and you will need 8-10 minutes to complete it. This survey is targeted at three primary groups: Cloud Services Buyers (organizations or users that have adopted or looking forward to adopt cloud solutions); Cloud Service Providers (providers of cloud solutions, including independent software vendors or ISVs and service providers); and Cloud Advisors (consultants and third-party advisors who work with cloud buyers and provide guidance on cloud adoption strategies).

Participation
In return for the contributions, participants will receive a summary of the research findings once analysed, together with an e-copy of the final research results once published in an academic journal.

Privacy Statement
All information provided by respondents will be strictly confidential (individuals will not be identified) and will be purely used for academic purposes. Data collected will be kept securely. Participation is completely voluntary and you may stop and leave at any time.

In order to progress through the survey, please use the following navigation links:

Continue to the next page of the survey by clicking the *Continue to the Next Page* >>

Go back to the previous page in the survey by clicking on the *Previous Page* << link.

Finish the survey, by clicking the *Submit the Survey* >> link.

Appreciation
I would like to thank you very much in advance for kindly agreeing to participate in this survey. Should you have any questions or comments about this study or the questionnaire please contact the researcher *(Justice Opara-Martins)* using the information below.

Many thanks.

Justice Opara-Martins (AMBCS)

Doctoral Researcher
Faculty of Science and Technology
Bournemouth University
P517B, Poole House
Talbot Campus, Fern Barrow
Poole, Dorset, BH12 5BB
United Kingdom

Tel: +44 (0) 1202 961326
Mobile: +44 (0) 776 585 6758
Email: joparamartins@bournemouth.ac.uk

Understanding How Vendor Lock-In Impacts on Adoption of Cloud Computing

Organisational Demography

***1. Which industry best describes your organization?**

***2. What is the size of your organization?**

- 1-24 Employees
- 25-50 Employees
- 51-250 Employees
- 251-500 Employees
- 501-1000 Employees
- Over 1000 Employees

***3. Your Department**

- Accounting
- Administration
- Finance
- Human Resource
- IT
- Logistics / Warehouse
- Marketing / Sales
- Operations
- Procurement
- Research and Development

Other

***4. Which of the following people in your organization are making buying decisions on cloud services? (Please check all that apply)**

- [ ] CEO
- [ ] IT Management
- [ ] CIO
- [ ] CTO
- [ ] Business Line Manager

Other (please specify)

Business View on Cloud Computing

5. Which of the following best describes the adoption of cloud computing in your organization?

- ☐ We are already using cloud services
- ☐ We utilize combination of cloud services and internally owned applications for organization needs
- ☐ We expect to adopt cloud services within the upcoming 12 months
- ☐ We have no intention to adopt cloud computing

*6. The reasons behind using cloud computing services in your organization are? (Please check all that apply)

- ☐ Better scalability of IT resources
- ☐ Collaboration
- ☐ Cost savings
- ☐ More flexibility
- ☐ Risk management
- ☐ Improve security
- ☐ Increase storage capacity
- ☐ Greater IT efficiency and agility
- ☐ Business continuity, regular backups, and disaster recovery capabilities
- ☐ Adding redundancy to network infrastructure to increase availability and resilience

Other (please specify)

***7. What does your organization view as the most important benefits of cloud computing? (Please check/enter top 3 from the list)**

- ☐ Pricing flexibility
- ☐ Increased collaboration
- ☐ Reduced infrastructure cost
- ☐ Security and Backup
- ☐ Capacity, scalability and speed
- ☐ Availability, geography and mobility
- ☐ Increased business agility and greater productivity
- ☐ Business Intelligence (BI)
- ☐ Competitiveness
- ☐ Other (please specify)

***8. What are the greatest barriers for implementing cloud computing in your organization? (Please check all that apply)**

- ☐ System and data security risks
- ☐ Over dependence on a single cloud provider
- ☐ Legal and regulatory compliance issues
- ☐ Data access and incompatibility issues
- ☐ Lack of integration between various cloud networks
- ☐ Data protection, privacy and other jurisdictional issues
- ☐ Implementation/transition/integration costs are too high
- ☐ Loss of control (system availability and business continuity risks etc)
- ☐ Inability to move data from one vendor to another or back onto our IT infrastructure
- ☐ We don't have cloud experts on staffs to implement a private or hybrid cloud

Other (please specify)

***9. Are you considering moving business critical systems (or applications) to the cloud?**

- We have already moved one or more of our business critical systems to the cloud
- We plan to move one or more of our business critical systems to the cloud in the upcoming 12 months
- Perhaps, but not within 12 months
- We have no considerations to move business critical systems to the cloud

Other (please specify)

Vendor Lock-In Risk Assessment and Management

***10. How important is it for your organization to integrate existing (on-premise) IT asset with cloud-based services?**

- Extremely important
- Very important
- Moderately important
- Slightly important
- Not at all important

Other (please specify)

***11. How would you express your current understanding of the term "Vendor Lock-In" in cloud computing context?**

- Excellent understanding
- Good understanding
- Basic understanding
- Poor understanding
- No understanding

***12. "Vendor lock-in in cloud computing is the situation in which customers (i.e. businesses and end-users) are dependent on a single cloud providers technology solution or service and cannot easily move in the future to another cloud offering from a different vendor without substantial costs and/or inconvenience".**

Based on the definition above, do concerns about Vendor Lock-in deter your organization from adopting cloud services?

- Definitely yes
- Possibly yes
- No
- Not sure

***13. Please identify which interoperability or data portability issues you have encountered when using cloud services OR are otherwise aware of. (Please check/enter all that apply)**

- ☐ Inability to pool services from different providers
- ☐ Authentication and authorisation issues
- ☐ Issues with compliance of security policies and procedures
- ☐ Virtual machine management (provision, contextualisation, de-provision) issues
- ☐ Proprietary data format (incompatibility issues with existing software)
- ☐ Inability to move to another service provider or take data in-house
- ☐ Lack of integration points with existing management tools
- ☐ Data management and access challenges

Other (please specify)

***14. From your perspective, which existing or emerging standards support Interoperability across the cloud and Portability of data (from one cloud provider to another)?**

- [ ] Open Cloud Computing Interface (OCCI)
- [ ] Open Data Protocol (OData)
- [ ] Distributed Management Task Force (DMTF) Cloud Data Management Interface (CDMI)
- [ ] DMTF's Open Virtualization Format (OVF)
- [ ] International Standards Organisation (ISO) CDMI
- [ ] Unified Cloud Interface (UCI)
- [ ] Cloud Computing Interoperability Forum (CCIF)
- [ ] CTP – Cloud Trust protocol
- [ ] OpenStack
- [ ] IEEE P2301 and P2302 Standards for cloud-to-cloud interoperability and portability
- [ ] Not sure

Other (please specify)

***15. To the best of your knowledge, how can the risks of Vendor Lock-in be minimised in cloud computing environment?**

- [ ] Use standard software components with industry-proven interfaces
- [ ] Ensure application architectures and IT operations procedures that are not unique to a specific vendor platform
- [ ] Considerations for the use of open and published technologies (standardisation)
- [ ] Practice and conduct due diligence when hiring cloud providers
- [ ] Well-informed decisions before selecting vendors and/or signing the cloud service contract
- [ ] Build perceived lock-in risks into initial risk assessment and mitigate by choosing a vendor with limited risks
- [ ] Involve legal teams and security professional when negotiating cloud providers contract terms and SLA
- [ ] An open environment of continuous competition between providers in the cloud services market
- [ ] Not sure

Other (please specify)

Organization Strategic Approach to Cloud Utilization

***16. Typical cloud computing services are classified into three main categories; Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS), and Software-as-a-Service (SaaS) as explained below.**

Which of these types of cloud computing is your organization currently using?

- ☐ IaaS provides resources such as compute, storage and communication services (e.g. include Amazon EC2, Rackspace, Google Compute Engine etc.)
- ☐ PaaS provides services such as complete operating system, software packages for application development and deployment on-demand (e.g. Windows Azure, Force.com, Google App Engine etc.)
- ☐ SaaS services include Salesforce CRM, Google Apps (like Google Docs and Spreadsheets), Microsoft Office 365, Cisco WebEx etc.

Other (please specify)

***17. Which of the following cloud types has your organization adopted?**

- ☐ Private cloud (internally owned and operated solely for a particular organization)
- ☐ Public cloud (accessible over the Internet, operated and managed by a third-party cloud vendor)
- ☐ Hybrid cloud (combination of private and public cloud to permit data and application portability)
- ☐ Community cloud (shared among several organizations with similar concerns relating to policy, compliance etc.)

Other (please specify)

***18. Did your organization negotiate a cloud service contract/service level agreement (SLA) rather than accepting the cloud provider's standard terms of service?**

- ○ Yes
- ○ No
- ○ Not sure

***19. Does your organization have an exit strategy (i.e. a strategy to exit from one cloud provider to another or back in-house) upon termination of cloud service contract?**

- ○ Yes there is an exit strategy in case of contract termination
- ○ Yes, but there are no agreed ownership rights of all data that will be stored in the cloud
- ○ Don't know
- ○ No

Other (please specify)

***20. To the best of your knowledge, when negotiating with a cloud service provider which of the following agreements should be included in the contract/SLA? (Please check all that apply)**

- ☐ Quality of Service (QoS) guarantee (service availability; uptime & downtime)
- ☐ Security (network and physical security requirements)
- ☐ Intellectual Property (IP) rights
- ☐ Data Protection (data and metadata ownership, security, location of data, E-discovery, backup and recovery etc.)
- ☐ Laws and Jurisdiction (regulatory and legal compliance)
- ☐ Warranties & Indemnities
- ☐ Exclusions and limitations of liability (for data outages and data loss)
- ☐ Transition out (data export functionality)
- ☐ Contract termination (retention and destruction of data)

Other (please specify)

***21. Which one of the following applications are currently using cloud services in your organization?**

	Already adopted cloud	Considered moving to cloud	Do not intend to adopt cloud
Desktop & Office software	○	○	○
Email & Messaging	○	○	○
BPM - Business Process Management	○	○	○
ERP / Enterprise management	○	○	○
CRM / Customer management	○	○	○
Accounting and finance	○	○	○
Application development platform	○	○	○
Disaster recovery applications	○	○	○
Business Intelligence (BI)	○	○	○
Content Management Systems (CMS)	○	○	○

Understanding How Vendor Lock-In Impacts on Adoption of Cloud Computing

***22. The following are some of the unfavorable outcomes (or risks) of vendor lock-in in cloud computing. How critical are each one of these risks to your organisation's business operation and processes. Please rate each risk using a scale of 0-3, with 3 being the highest (n.b. a choice is needed for all options).**

	(0) Not critical	(1) Low	(2) Moderate	(3) Critical
Having my data locked-in to one cloud provider	○	○	○	○
Data breach and cyber attack	○	○	○	○
Costly data migration or data conversion	○	○	○	○
Failure to provide agreed service/meet service levels	○	○	○	○
The lack of integration between various cloud networks	○	○	○	○
Unexpected application re-engineering or business process change	○	○	○	○
Processing incompatibility and conflicts causing disruption of service	○	○	○	○
Inability to easily move data and applications in/out of cloud environments	○	○	○	○

***23. How likely do you consider using a cloud-based Vendor Risk Management solution if such a strategy allowed your business to understand and manage vendor lock-in risks and compliance requirements effectively?**

- Extremely likely
- Quite likely
- Moderately likely
- Slightly likely
- Not at all likely

Other (please specify)

***24. To the best of your knowledge, what skills should be in place for proper cloud computing services implementation and migration?**

- [ ] Information security analyst skills
- [ ] Integration specialist and cloud architects
- [ ] Network administration and engineering skills
- [ ] Virtualization skills
- [ ] Project management skills
- [ ] Contract and vendor negotiation skills
- [ ] Good understanding of data protection laws and regulation
- [ ] Knowledge in the legal, compliance, security and risk management issues in cloud computing
- [ ] Enhanced technical knowledge and understanding of cloud computing
- [ ] Need for more specialised set of skills
- [ ] Not sure

Other (please specify)

Cloud Computing Security and Data Privacy Risk Assessment

***25. To what extent does geographical location matter in regard to where your organization data is stored?**

- Location completely matters
- Location matters somewhat
- Location does not matter at all
- Don't know

Other (please specify)

***26. How concerned, if at all, are you about the security of your organization data in cloud storage?**

- Very concerned
- Fairly concerned
- Not very concerned
- Not at all concerned
- Don't know

***27. Using a scale of 1 to 5, with 5 being the highest. Please rate the following options in order of where you believe your organisation data would be safest (n.b. a choice is needed for all options).**

	(1) Poor	(2) Fair	(3) Good	(4) Very Good	(5) Excellent
With a cloud provider located in the UK	○	○	○	○	○
They don't have to be located in the UK, but have to be in Europe (EEA)	○	○	○	○	○
On your own hardware in a shared data center (colocation)	○	○	○	○	○
A cloud run by a company with reputation of trustworthiness	○	○	○	○	○
On your own hardware with your own facilities	○	○	○	○	○
They can be located anywhere in the world	○	○	○	○	○

***28. Thank you for taking the time and effort to complete this survey. Would you like to receive a copy of the research results/findings?**

- ○ Yes
- ○ No

If you answered yes, please enter contact details (e.g. email, phone, etc).

APPENDIX 5

Influences and Relations with Decision Steps

	Step 6.5 – Post migration Support	Step 6.4 – Decommissioning	Step 6.3 – Customer audit rights	Step 6.2 – Monitoring and organisational change management	Step 6.1 – System go-live	Decision Step 6 – Service Operation and Optimization	Step 5.5 – SaaS validation testing	Step 5.4 – SaaS security testing	Step 5.3 – Perform business testing	Step 5.2 – Conduct functional and non-functional SaaS testing	Step 5.1 – Build an in-house SaaS test team	Decision Step 5 – Service Testing and Validation	Step 4.4 – Conduct migration	Step 4.3 – Provide cloud resources	Step 4.2 – Select the migration scenario	Step 4.1 – Assess the complexity of migration	Decision Step 4 – Design and Execute the Migration Plan	Step 3.5 – Review, accept and sign final contract/SLA	Step 3.4 – Get internal approval	Step 3.3 – Agree draft of ToS/SLA	Step 3.2 – Carryout negotiation	Step 3.1 – Establish a negotiation team	Decision Step 3 – Contract Negotiation and SLA	Step 2.4 – Devise a cloud vendor adoption principle	Step 2.3 – Evaluate vendor(s) against defined criteria	Step 2.2 – Conduct due diligence on potential vendors	Step 2.1 – Define evaluation criteria	Decision Step 2 – Vendor Evaluation and Selection	Step 1.5 – SaaS Risk assessment and mitigation	Step 1.4 Establish SaaS governance model and adoption principle	Step 1.3 – SaaS application suitability	Step 1.2 -Requirement Analysis	Step 1.1 – Define organisation context	Decision Step 1 – Initial Migration Panning
LEGEND: I represent" Influences"; D represent "Determines"																																		
Decision Step 1 – Initial Migration Panning				I				D							I					I														
Step 1.1 – Define organisation context					I	I	I																			I							I	I
Step 1.2 – Requirement Analysis																										I								
Step 1.3 – SaaS application suitability																										I								
Step 1.4 Establish SaaS governance model and adoption principle				I	I																					I								I
Step 1.5 – SaaS Risk assessment and mitigation																				I						I								I
Decision Step 2 – Vendor Evaluation and Selection														I												I						D		I
Step 2.1 – Define evaluation criteria																										I		I		I			I	
Step 2.2 – Conduct due diligence on potential vendors				I																			I	I	I									
Step 2.3 – Evaluate vendor(s) against defined criteria																								I	I				I	D				
Step 2.4 – Devise a cloud vendor adoption principle		I																						I	I									
Decision Step 3 – Contract Negotiation and SLA							I						I														D				I	D		
Step 3.1 – Establish a negotiation team																						I	I											
Step 3.2 – Carryout negotiation		I																																
Step 3.3 – Agree draft of ToS/SLA																		I														I	I		I
Step 3.4 – Get internal approval						I														I	I													
Step 3.5 – Review, accept and sign final contract/SLA																			I	I	I													
												I																							
Decision Step 4 – Design and Execute the Migration Plan		I					D						I		I										I							D		
Step 4.1 – Assess the complexity of migration																																		
Step 4.2 – Select the migration scenario																	D										I						I	
Step 4.3 – Provide cloud resources																I	D				D													
Step 4.4 – Conduct migration																I	D																	
Decision Step 5 – Service Testing and Validation								D				I	I		D			I															D		
Step 5.1 – Build an in-house SaaS test team									I																									
Step 5.2 – Conduct functional and non-functional SaaS testing												I																						
Step 5.3 – Perform business testing					I							I																						
Step 5.4 – SaaS security testing					I							I																						
Step 5.5 – SaaS validation testing												I																						
Decision Step 6 – Service Operation and Optimization													I					I															D		
Step 6.1 – System go-live					D																													
Step 6.2 – Monitoring and organisational change management						I																											I		D
Step 6.3 – Customer audit rights											I							D									I							
Step 6.4 – Decommissioning						I																												
Step 6.5 – Post migration support					D															D														I

APPENDIX 6

The Framework Evaluation Questionnaire

A Decision Framework to Avoid Vendor Lock-in Risks in Cloud Migration

About this Questionnaire

Dear Sir / Madam

Thank you for participating in this survey. This questionnaire is being conducted for a PhD research. Prior to this questionnaire, previous research survey was carried out (by author) to investigate the business related risks of vendor lock-in affecting the adoption of cloud services by organisations. As a result of the initial research study, a framework to avoid vendor lock-in when migrating/adopting cloud based services has been developed. Therefore, the ultimate goal of this questionnaire is to seek IT experts and cloud practitioners' views on the suitability of the proposed framework to guide and support enterprise decisions for avoiding vendor lock-in risks. The questionnaire compromises of 25 short questions and you will need no more than **15 minutes** to complete it.

Survey Outcome

Participants will receive a summary of the analysis of the findings, together with an email of the final research results.

Privacy Statement

All information provided by respondents will be strictly confidential (individuals will not be identified) and will be purely used for academic purposes. Data collected will be kept securely. Participation is completely voluntary and you may stop and leave at any time.

Proposed Framework Diagram(s)

Diagrams illustrating the proposed framework can be found in section(s) B-D of this questionnaire. The framework diagrams illustrate the steps, phases, and tasks to be carried out to avoid vendor lock-in for cloud-based services (SaaS category) migration. Since revealing the full details of each step will provide overwhelming information, for the purpose of this questionnaire only the details of Step 2 decision trees are provided (as examples) for information purpose.

Appreciation

I would like to thank you very much in advance for kindly agreeing to participate in this survey. Should you have any questions or comments about this study or the questionnaire please contact the researcher (**Justice Opara-Martins**) using the information below.

Many thanks.
Signed:
Justice Opara-Martins (AMBCS)

Doctoral Researcher in Cloud Computing
Center for Games and Music Technology Research
Faculty of Science and Technology
Bournemouth University
P517B, Poole House
Talbot Campus, Fern Barrow
Poole, Dorset, BH12 5BB
United Kingdom

Tel: +44 (0) 1202 961326
Mobile: +44 (0) 776 585 6758
Email: joparamartins@bournemouth.ac.uk

Section A: General Questions to the Respondents

1. Please enter your organisation name below (optional)

* 2. Which of the following most closely matches your job title?

- ○ IT Professional
- ○ Manager
- ○ Cloud Architect
- ○ Cloud Developer
- ○ C level executive (CIO, CTO, COO, CFO etc.)
- ○ Other (please specify)

* 3. What is the highest level of school you have completed or the highest degree you have received?

- ○ Less than high school degree
- ○ High school degree or equivalent
- ○ Some college but no degree
- ○ Associate degree
- ○ Bachelor degree
- ○ Graduate or professional degree
- ○ Ph.D

* 4. What level of decision-making authority do you have on purchasing IT related hardware, software or services for your organisation?

- ○ Final decision-making authority (individually or as part of a group)
- ○ Significant decision-making or influence (individually or as part of a group)
- ○ Minimal decision-making or influence
- ○ No input

* 5. On a scale from 0-4, how much experience do you have with the following?

	No experience (0)	Poor experience (1)	Average experience (2)	Good experience (3)	Excellent experience (4)
Cloud Computing	○	○	○	○	○
IT Services	○	○	○	○	○
Cloud Computing Migration	○	○	○	○	○
Adoption of cloud-based services or software applications	○	○	○	○	○

A Decision Framework to Avoid Vendor Lock-in Risks in Cloud Migration

Section B: About the Framework

A decision framework to avoid vendor lock-in risks for migrating IT services to the cloud and adopting cloud-based services (SaaS) proposed by this research highlights the issues and actions. This include contractual matters which must be considered and implemented before adopting the services, or migrating from one SaaS provider to another. The framework through its step-by-step approach provides guidance on how to avoid being locked to individual cloud service providers. This reduces the risk of dependency on a particular cloud provider for service provision, especially if data portability, as the most fundamental aspect, is not enabled. Moreover, it also ensures appropriate pre-planning and due diligence so that the correct cloud service provider(s) with the most acceptable risks to vendor lock-in is chosen, and that the impact on the business is properly understood (upfront), managed (iteratively), and controlled (periodically).

Each decision step within the framework prepares the way for the subsequent step, which supports a company to gather the correct information to make a right decision before proceeding to the next step. The reason for such an approach is to support an organisation with its planning and adaptation of the services to suit the business requirements and objectives – so the sequence is important and should be followed for a successful outcome.

The main decision the framework supports refer to:

- how to select a cloud service provider and its offerings that fits the organisations needs in terms of contractual agreement, cost, expected performance based on compatibility, interoperability, portability and standards, compliance requirements and security concerns;

Two unique concepts of the framework are:

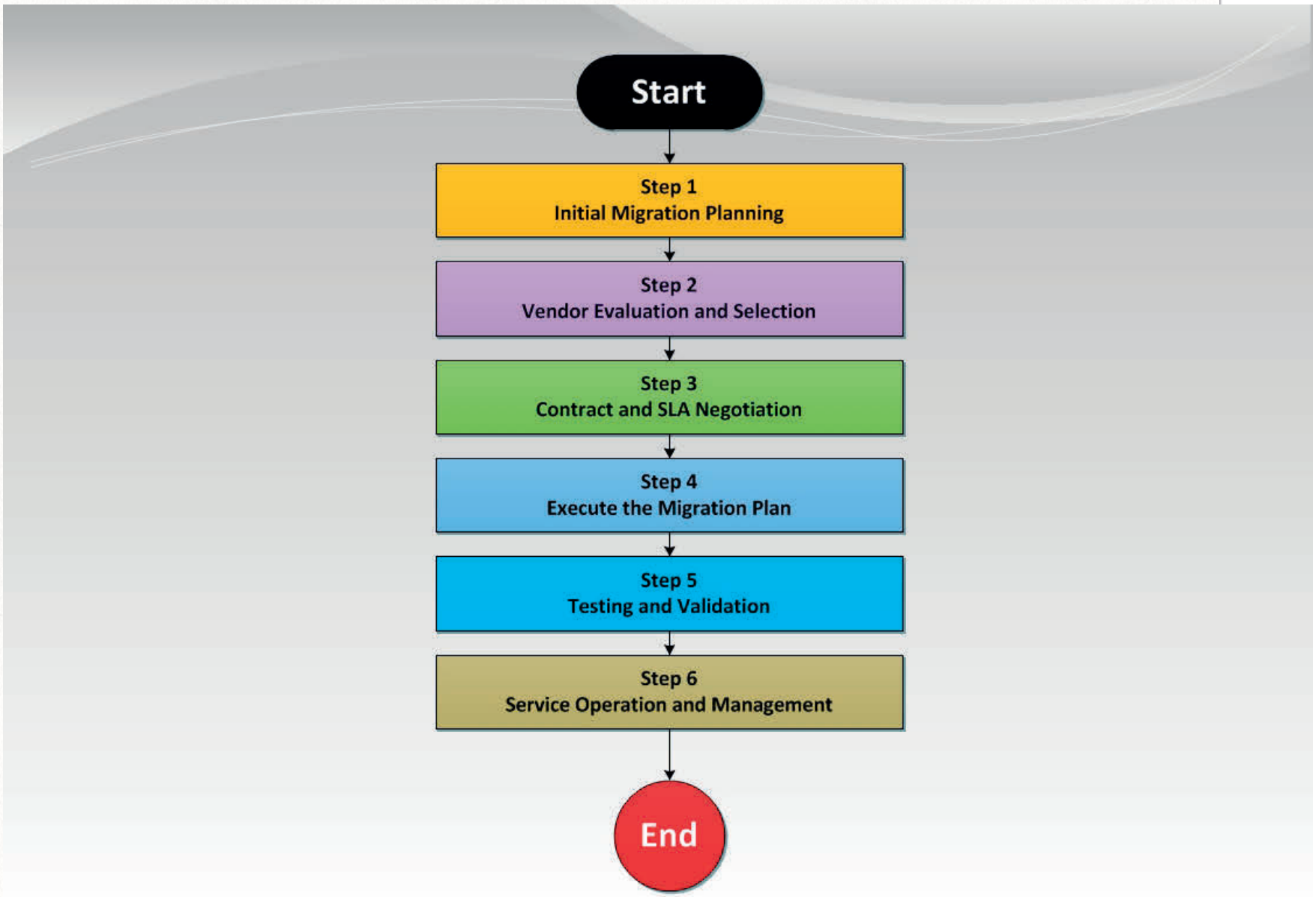
- decisions that need to be made, and
- tasks (or activities) that need to be performed in order to support these decisions which in turn affect their outcome (i.e. artefacts).

A Decision Framework to Avoid Vendor Lock-in Risks in Cloud Migration

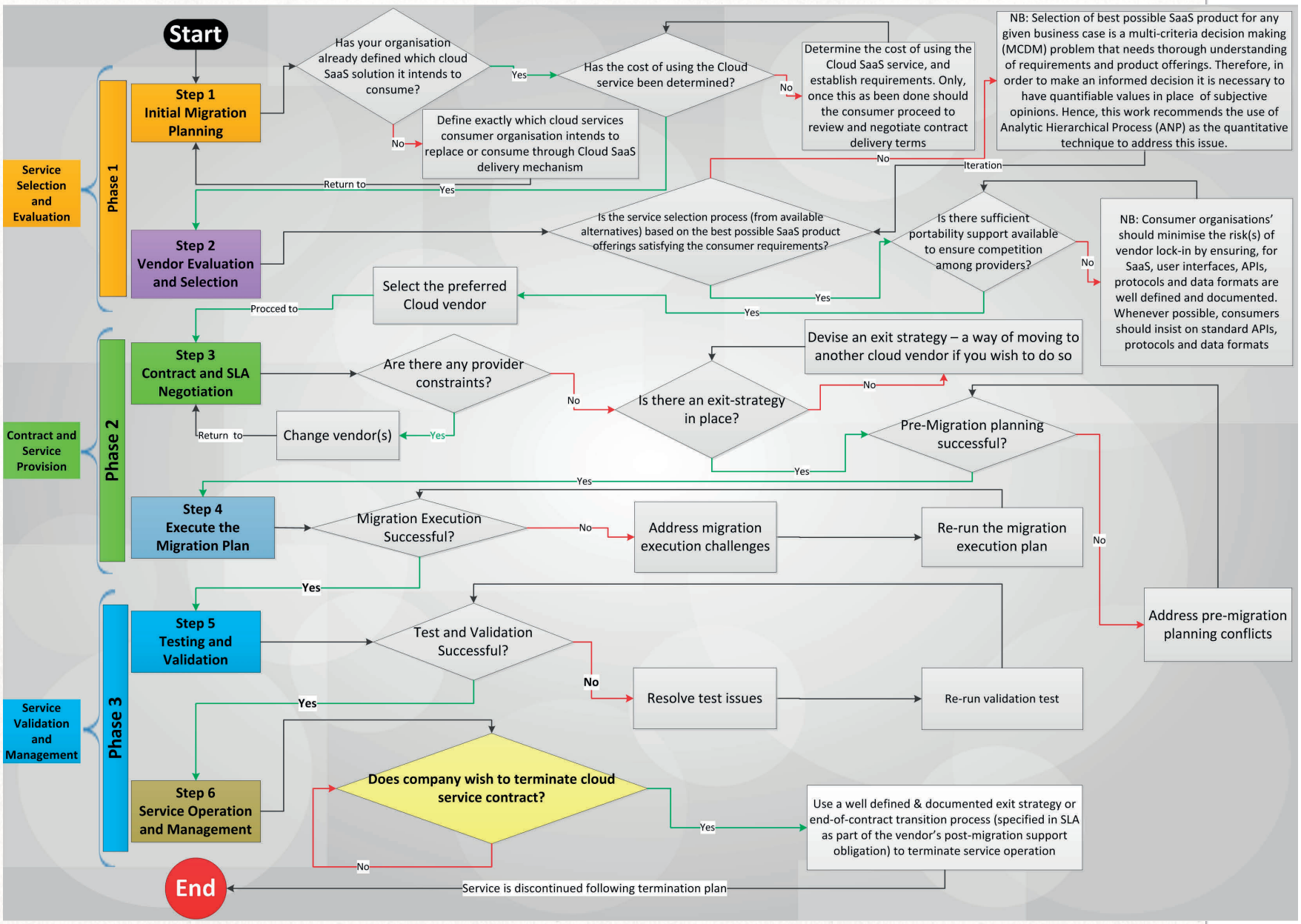
Section B (contd): Framework Diagrams

NB: The framework diagram(s) below shows the sequence and inter-relationship between the six main decision steps and their corresponding tasks/activities.

The 6-Step Decision Framework for Cloud Migration - A General Overview Diagram



Phase Diagram with Step-by-Step Decision Process Logic



A Decision Framework to Avoid Vendor Lock-in Risks in Cloud Migration

Section C: Evaluation of the Proposed Framework

In response to the diagrams provided in Section B, please respond to the following questions using the rating scale provided below to evaluate the proposed framework accordingly.

Scoring: On a scale from 0-4, rate the framework on the criteria listed below. Please provide comments which reflect suggestions for improvements and/or recommendation for items that are done well.

NOTE: Rating Scale for

Appropriateness: 0 = Not appropriate, 1 = Slightly appropriate, 2 = Moderately Appropriate, 3 = Very appropriate, 4 = Absolutely appropriate

Importance: 0 = Not at all important, 1 = Slightly important, 2 = Moderately important, 3 = Very important, 4 = Absolutely important

6. The following are steps within the framework that organisations should go through when migrating to Or switching cloud Software-as-a-Service (SaaS) providers to avoid vendor lock-in. If you do not agree with the **logical order**, please indicate the order that you wish to see in the framework.

- Step 1 - Initial Migration Planning
- Step 2 - Vendor Evaluation and Selection
- Step 3 - Contract Negotiation and Service Level Agreement (SLA)
- Step 4 - Design and Execute the Migration Plan
- Step 5 - Service Testing and Validation
- Step 6 - Service Operation and Optimization

* 7. Is the **logical order** within the framework *appropriate*? By logical order, we mean how reasonable or sensible the sequence of steps within the framework happens or should happen in a typical cloud migration project.

- Yes
- No

If you answered No, in your opinion what should be the correct order?

A Decision Framework to Avoid Vendor Lock-in Risks in Cloud Migration

Section D: Evaluating each Step and corresponding Tasks within the Framework

In response to the diagrams provided in Section B and C, please respond to the following questions using the rating scale provided below to evaluate the proposed framework accordingly.

Scoring: On a scale from 0-4, rate the framework on the criteria listed below. Please provide comments which reflect suggestions for improvements and/or recommendation for items that are done well.

NOTE: Rating Scale for

Appropriateness: 0 = Not appropriate, 1 = Slightly appropriate, 2 = Moderately Appropriate, 3 = Very appropriate, 4 = Absolutely appropriate

Importance: 0 = Not at all important, 1 = Slightly important, 2 = Moderately important, 3 = Very important, 4 = Absolutely important

* 8. Please rate how **appropriate** the steps (1-6) are to you in cloud migration strategy? By *appropriate*, we mean how suitable a step is for you. The more you feel the step is appropriate to you, the higher you would rate it. The less you feel the step is appropriate for you, the lower you would rate.

	0 (Not at all appropriate)	1	2	3	4 (Absolutely appropriate)
Step 1 - Initial Migration Planning	○	○	○	○	○
Step 2 - Vendor Evaluation and Selection	○	○	○	○	○
Step 3 - Contract Negotiation and SLA	○	○	○	○	○
Step 4 - Design and Execute the Migration Plan	○	○	○	○	○
Step 5 - Service Testing and Validation	○	○	○	○	○
Step 6 - Service Operation and Optimization	○	○	○	○	○

* 9. Please rate how **important** each step is to you in a cloud (Software-as-a-Service or SaaS) migration. By *importance*, we mean how relevant a step is for you. The more you feel the step is important to you, the higher you would rate it. The less you feel the step is important for you, the lower you would rate.

	0 (Not at all important)	1	2	3	4 (Absolutely important)
Step 1 - Initial Migration Planning	○	○	○	○	○
Step 2 - Vendor Evaluation and Selection	○	○	○	○	○
Step 3 - Contract Negotiation and Selection	○	○	○	○	○
Step 4 - Design and Execute the Migration Plan	○	○	○	○	○
Step 5 - Service Testing and Validation	○	○	○	○	○
Step 6 - Service Operation and Optimization	○	○	○	○	○

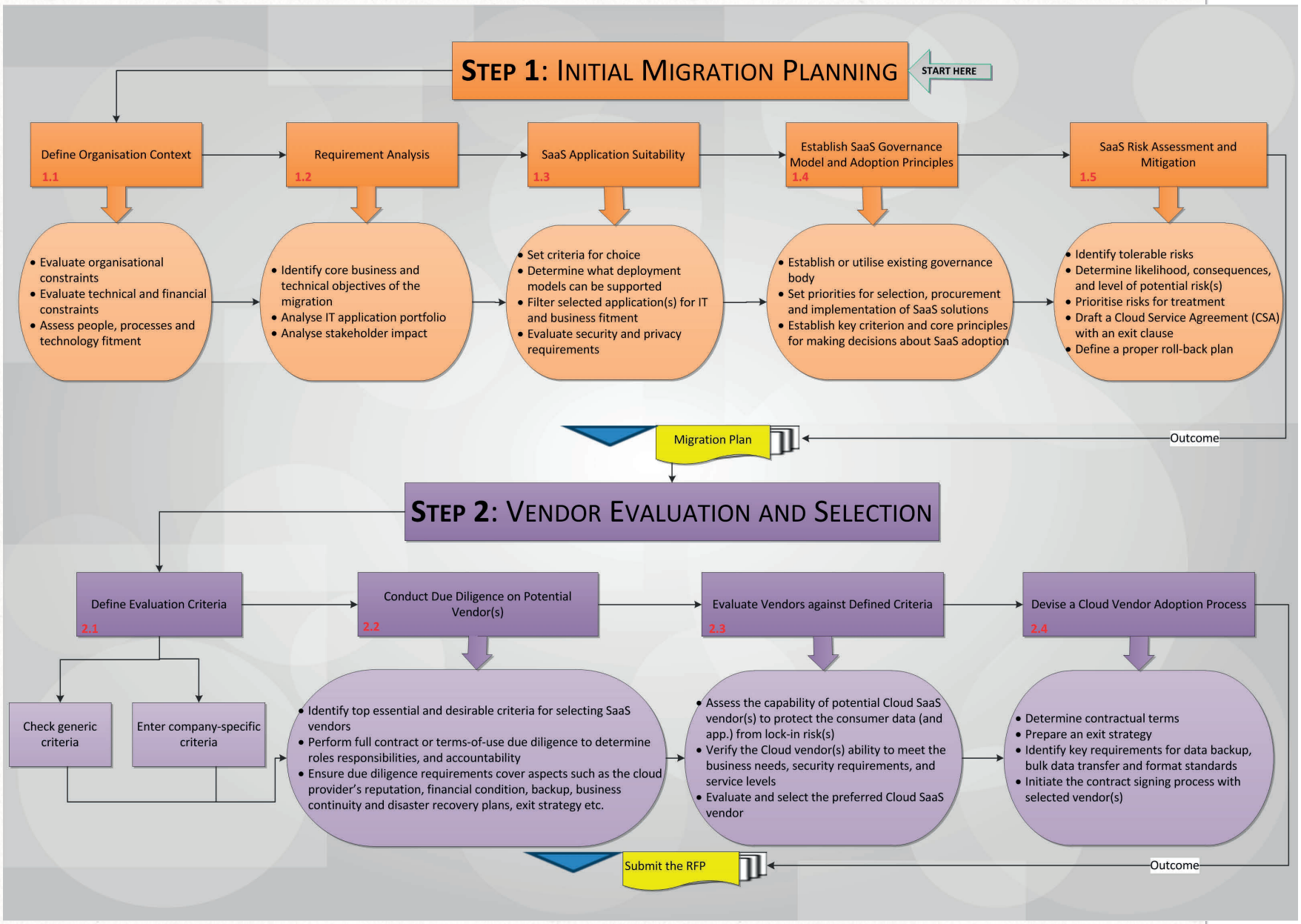
Other important attributes missing? (please specify here):

A Decision Framework to Avoid Vendor Lock-in Risks in Cloud Migration

Section D - Phase 1

Phase 1 mainly involves strategies for conducting effective business and IT requirement analysis to meet enterprise needs within efficient pricing, contracting, and security parameters, as well as procedures to engage cloud service providers in enabling portable and inter-operable cloud solutions. The output of Phase 1 is a detailed migration plan and road-maps for cloud deployment, service provider selection, and contract negotiation. These road-maps outlines series of activities required to move a SaaS application, and prioritize on-premise services that have high expected value and high readiness to maximise benefits received and minimize delivery risks of vendor lock-in.

Service Selection and Evaluation Phase (1)



* 10. Please rate the ***importance*** of each **task** to be performed during the initial migration planning (i.e. **Step 1**).

	0 (Not at all important)	1	2	3	4 (Absolutely important)
Step 1.1 - Define organisational context	○	○	○	○	○
Step 1.2 - Requirement analysis	○	○	○	○	○
Step 1.3 - SaaS application suitability	○	○	○	○	○
Step 1.4 - Establish SaaS governance model and adoption principles	○	○	○	○	○
Step 1.5 - SaaS risk assessment and mitigation	○	○	○	○	○

Is there any important attribute missing from the tasks in Step 1 above? Other (please specify here):

* 11. How **appropriate** are each ***task*** in Step 1?

	0 (Not at all appropriate)	1	2	3	4 (Absolutely appropriate)
Step 1.2 - Define organisational context	○	○	○	○	○
Step 1.2 - Requirement analysis	○	○	○	○	○
Step 1.3 - SaaS application suitability	○	○	○	○	○
Step 1.4 - Establish SaaS governance model and adoption principles	○	○	○	○	○
Step 1.5 - SaaS risk assessment and mitigation	○	○	○	○	○

* 12. Please rate the ***importance*** of each of the following **task** in **Step 2** (i.e. Vendor Evaluation and Selection).

	0 (Not at all important)	1	2	3	4 (Absolutely important)
Step 2.1 - Define evaluation criteria	○	○	○	○	○
Step 2.2 - Conduct due diligence	○	○	○	○	○
Step 2.3 - Evaluate vendors against defined criteria	○	○	○	○	○
Step 2.4 - Devise a cloud vendor adoption process	○	○	○	○	○

Is there any important attribute missing from the tasks in Step 2 above? If any, please specify here:

* 13. How **appropriate** are each ***task*** in Step 2?

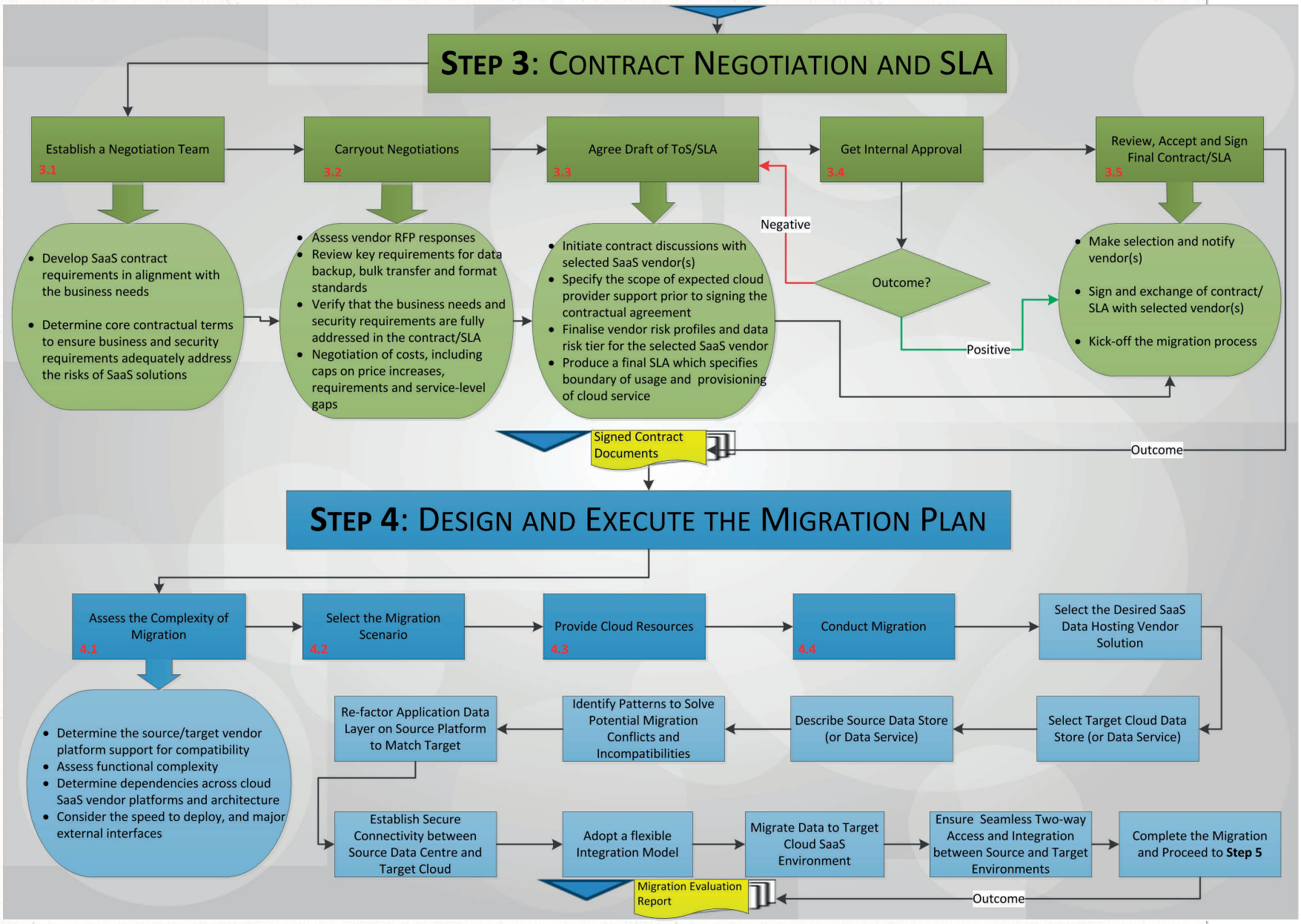
	0 (Not at all appropriate)	1	2	3	4 (Absolutely appropriate)
Step 2.1 - Define evaluation criteria	○	○	○	○	○
Step 2.2 - Conduct due diligence	○	○	○	○	○
Step 2.3 - Evaluate vendors against defined criteria	○	○	○	○	○
Step 2.4 - Devise a cloud vendor adoption process	○	○	○	○	○

A Decision Framework to Avoid Vendor Lock-in Risks in Cloud Migration

Section D - Phase 2

In Phase 2, the actual migration of data and application component (i.e. business logic) is carried out, tested and evaluated to validate the migrated SaaS service performs as expected, and in accordance to the signed contract(s) by both parties. To be successful in Phase 2, organisations must think carefully through a number of factors including interoperability and portability, security, capability to integrate services, strategies to contract effectively and realize value.

Contract and Service Provision Phase (2)



* 14. Please rate the ***importance*** of each **task** to be performed in **Step 3** (i.e.Contract Negotiation and SLA).

	0 (Not at all important)	1	2	3	4 (Absolutely important)
Step 3.1 - Establish a negotiation team	○	○	○	○	○
Step 3.2 - Carryout negotiations	○	○	○	○	○
Step 3.3 - Agree draft of ToS/SLA	○	○	○	○	○
Step 3.4 - Get internal approval	○	○	○	○	○
Step 3.5 - Review, accept and sign final contract/SLA	○	○	○	○	○

Is there any important attribute missing from the tasks in Step 3 above? Other (please specify here):

* 15. How **appropriate** are each ***task*** in Step 3?

	0 (Not at all appropriate)	1	2	3	4 (Absolutely appropriate)
Step 3.1 - Establish a negotiation team	○	○	○	○	○
Step 3.2 - Carryout negotiations	○	○	○	○	○
Step 3.3 - Agree draft of ToS/SLA	○	○	○	○	○
Step 3.4 - Get internal approval	○	○	○	○	○
Step 3.5 - Review, accept and sign final contract/SLA	○	○	○	○	○

* 16. Please rate the ***importance*** of each **task** to be performed in **Step 4** (i.e.Design and Execute the Migration Plan).

	0 (Not at all important)	1	2	3	4 (Absolutely important)
Step 4.1 - Assess the complexity of migration	○	○	○	○	○
Step 4.2 - Select the migration scenario	○	○	○	○	○
Step 4.3 - Provide cloud resources	○	○	○	○	○
Step 4.4 - Conduct the migration	○	○	○	○	○

Is there any important attribute missing from the tasks in Step 4 above? Other (please specify here):

* 17. How **appropriate** are each ***task*** in Step 4?

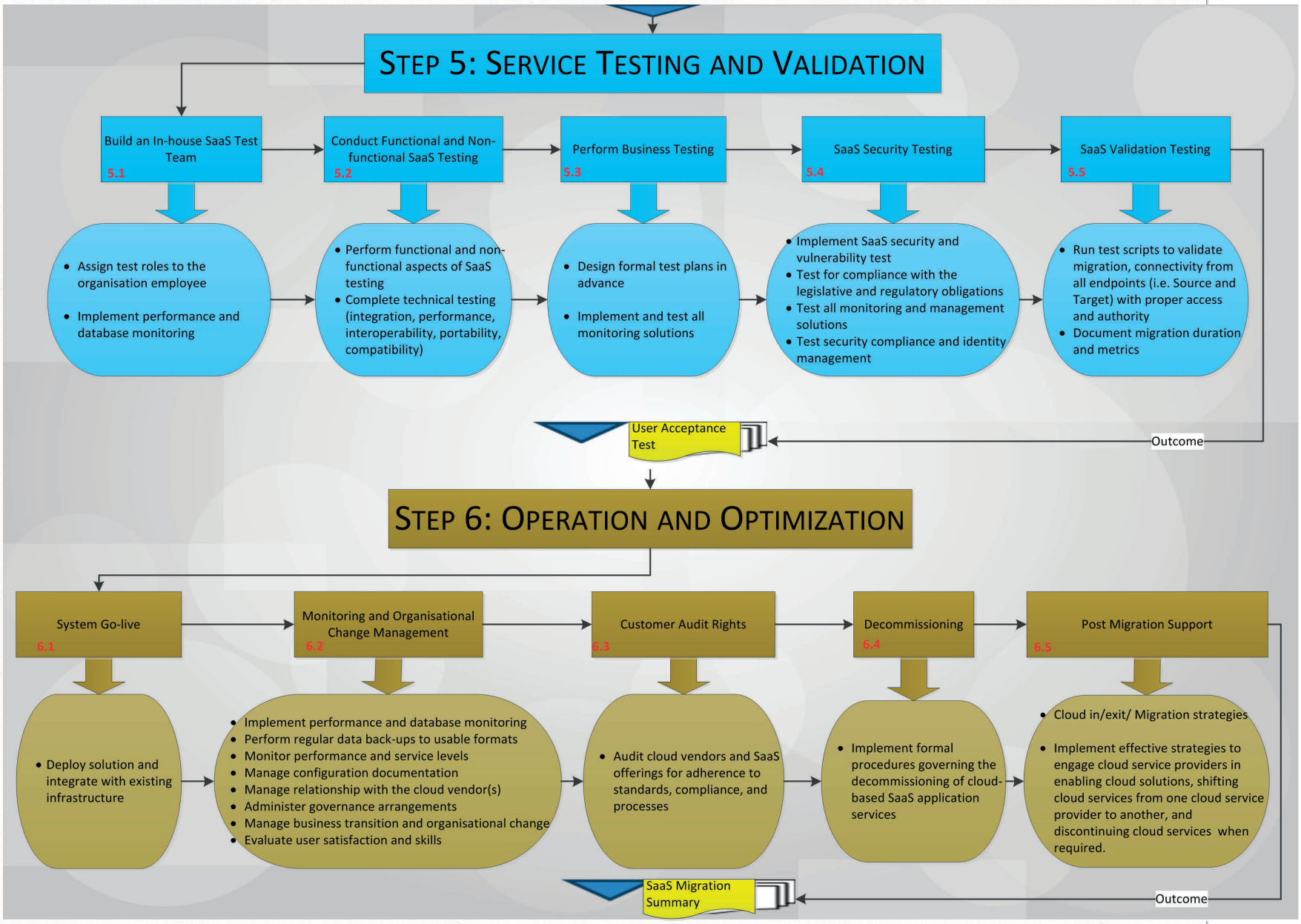
	0 (Not at all appropriate)	1	2	3	4 (Absolutely appropriate)
Step 4.1 - Assess the complexity of migration	○	○	○	○	○
Step 4.2 - Select the migration scenario	○	○	○	○	○
Step 4.3 - Provide cloud resources	○	○	○	○	○
Step 4.4 - Conduct the migration	○	○	○	○	○

A Decision Framework to Avoid Vendor Lock-in Risks in Cloud Migration

Section D - Phase 3

Phase 3 is required to maintain, monitor, optimise and manage the migrated SaaS service. The output of this phase defines compliance agreements, metrics to ensure required QoS is maintained and monitored, and effective attributes to engage service providers in discontinuing or terminating contracted cloud SaaS services when required with minimum or no lock-in effect. To be successful in phase 3, enterprises must view cloud computing with a new way of thinking that reflects a service-based focus rather than an asset-based focus.

Service Validation and Management Phase (3)



* 18. Please rate the ***importance*** of each **task** to be performed in **Step 5** (i.e. Service Testing and Validation)

	0 (Not at all important)	1	2	3	4 (Absolutely important)
Step 5.1 - Build an in-house SaaS test team	○	○	○	○	○
Step 5.2 - Conduct functional and non-functional SaaS testing	○	○	○	○	○
Step 5.3 - Perform business testing	○	○	○	○	○
Step 5.4 - Security testing	○	○	○	○	○
Step 5.5 - SaaS validation test	○	○	○	○	○

Is there any important attribute missing from the tasks in Step 5 above? Other (please specify here):

* 19. How **appropriate** are each ***task*** in Step 5?

	0 (Not at all appropriate)	1	2	3	4 (Absolutely appropriate)
Step 5.1 - Build an in-house SaaS test team	○	○	○	○	○
Step 5.2 - Conduct functional and non-functional SaaS testing	○	○	○	○	○
Step 5.3 - Perform business testing	○	○	○	○	○
Step 5.4 - Security testing	○	○	○	○	○
Step 5.5 - SaaS validation test	○	○	○	○	○

* 20. Please rate the ***importance*** of each **task** to be performed in **Step 6** (i.e. Service Operation and Validation).

	0 (Not at all important)	1	2	3	4 (Absolutely important)
Step 6.1 - System go-live	○	○	○	○	○
Step 6.2 - Monitoring and organisational change management	○	○	○	○	○
Step 6.3 - Decommissioning	○	○	○	○	○
Step 6.4 - Customer audit rights	○	○	○	○	○
Step 6.5 - Post migration support	○	○	○	○	○

Is there any important attribute missing from the tasks in Step 6 above? Other (please specify here):

* 21. How **important** are each ***task*** in Step 6?

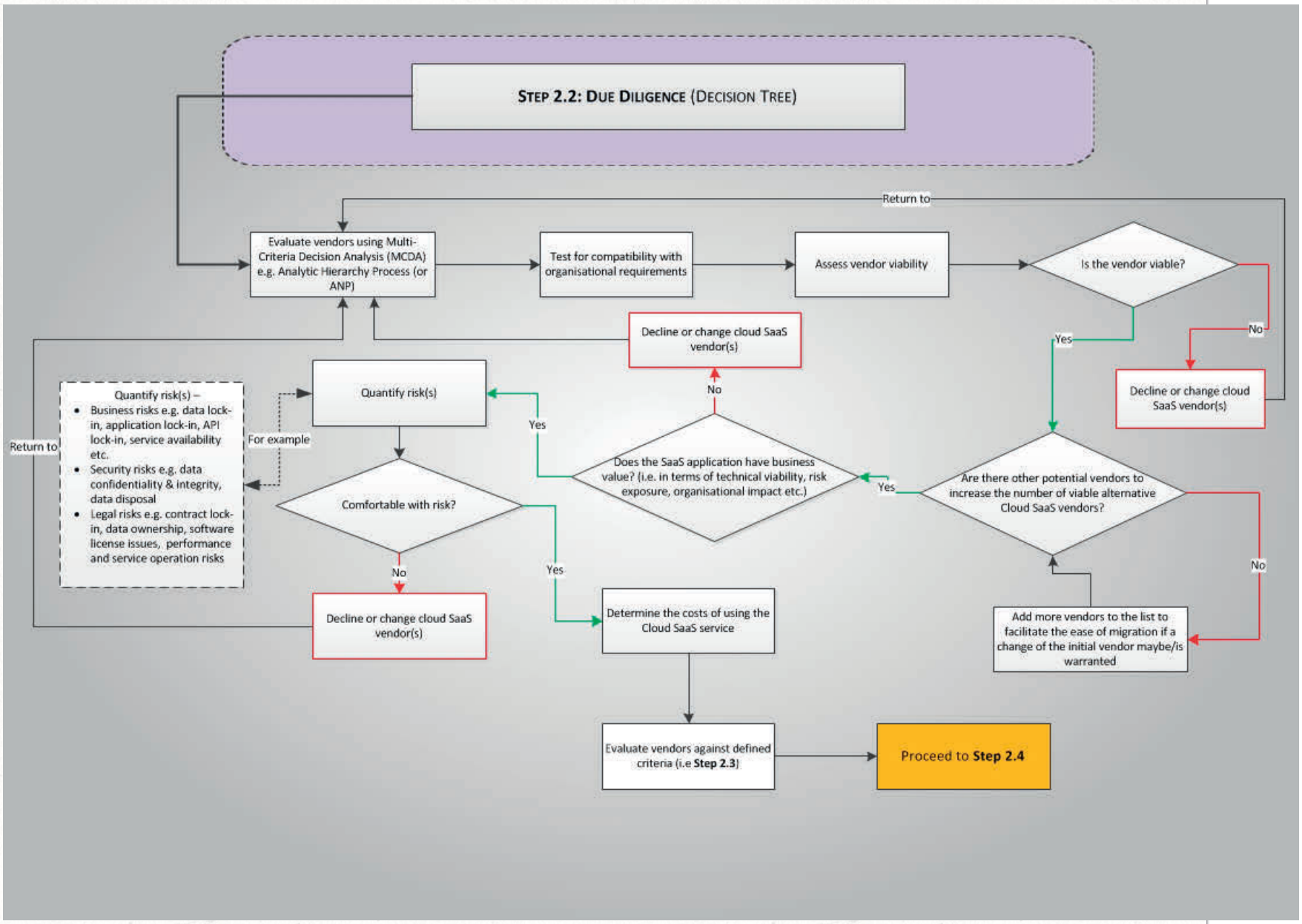
	0 (Not at all appropriate)	1	2	3	4 (Absolutely appropriate)
Step 6.1 - System go-live	○	○	○	○	○
Step 6.2 - Monitoring and organisational change management	○	○	○	○	○
Step 6.3 - Decommissioning	○	○	○	○	○
Step 6.4 - Customer audit rights	○	○	○	○	○
Step 6.5 - Post migration support	○	○	○	○	○

A Decision Framework to Avoid Vendor Lock-in Risks in Cloud Migration

Bournemouth University

Section E: Evaluating the sample Decision Trees for Step (2.2 & 2.4)

Step 2.2 - Due Diligence (Decision Tree)



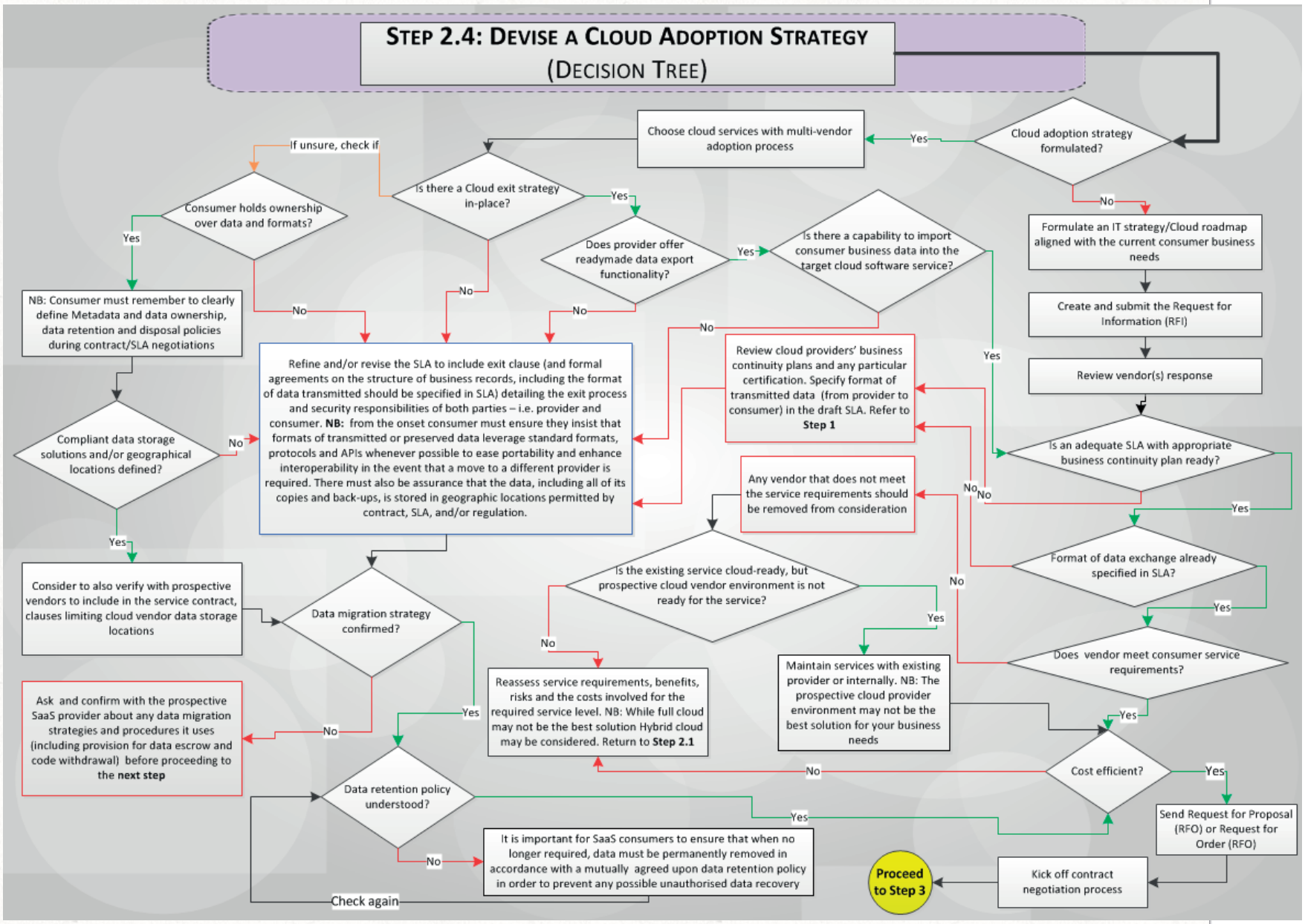
* 22. Step 2 was selected as an example to provide details of components within the *tasks* and relationship between them. The figure above is a decision tree sample illustrating details of tasks (and activities) within Step (2.2).

Does the **decision tree** above provide a good reflection of the *tasks* which are carried out in Step **2.2**?

- ○ Yes
- ○ No

If you answered No, what do you think is missing out? Please enter a comment here:

Step 2.4 - Devise a Cloud Adoption Strategy (Decision Tree)



* 23. Is the **decision tree** for Step **2.4** an accurate representation of the *tasks* and relationships between the components in Step 2?

- ○ Yes
- ○ No

If you answered No, what do you think is missing? Please add your comment here:

A Decision Framework to Avoid Vendor Lock-in Risks in Cloud Migration

Bournemouth University

Section F: Final Remarks

In response to the diagrams provided in Section**B-E**, please respond to the following questions using the rating scale provided below to evaluate the proposed framework accordingly.

NOTE: Rating Scale for

Effectiveness: 0 = Not at all effective, 1 = Slightly effective, 2 = Moderately effective, 3 = Very effective, 4 = Absolutely effective

By **effective,** we mean how positively or negatively you think or feel the framework will support cloud migration decisions. The more positively you regard the framework, the higher you would rate it. The more negatively you regard the framework, the lower you would rate. Having heard of cloud computing or cloud migration is enough for you to rate it.

24. Overall, how **effective** do you think this framework will be in supporting organisations' decision-making process for migration to cloud computing?

- ○ Extremely effective
- ○ Quite effective
- ○ Moderately effective
- ○ Slightly effective
- ○ Not at all effective.

25. Are there any comments/feedback's/suggestions which would help improve the framework? If any, please specify:

26. Please kindly indicate if you would like a copy of the research results/findings

- ○ Yes
- ○ No

If you answered yes, please enter contact (e.g. email, phone etc.) here:

APPENDIX 7

Analysis of Variance (One-Way ANOVA) Test Results for Framework Evaluation

Appendix 7

This appendix (abbreviated as Annex_7) is an extension of Chapter 6 as it presents the statistical test performed for each core component that is being evaluated within the proposed novel 6-step decision framework, based on an IT practitioners' viewpoint. Arguably, hypothesis testing is one of the most common methods used in statistical analysis. Hypothesis tests include two hypotheses (or claims), namely; 1) the null hypothesis (i.e. H_0) and, 2) the alternative hypothesis (H_1). The null hypothesis is the initial claim and is often specified based on previous research or common knowledge, whereas the alternative hypothesis is what is believed to be true.

Given the already analysed evaluation results presented in Chapter 6, based on basic (graphical) descriptive statistics, herein author performs a one-way ANOVA (including Tukey's multiple comparison test) to test the difference and equality of two or more means based on the results from Chapter 6. To perform this test, the evaluation questionnaire raw data is imported from survey monkey into MS Excel for data cleansing (i.e. identifying the means and standard deviation as the cohorts), and then into MiniTab for statistical data analysis. For each evaluated component within the framework, using the one-way ANOVA in MiniTab, weighted average (i.e. Mean) is the response, and standard deviation (or SD) is the factor as the two cohorts.

Performing One-Way ANOVA

In Fig.A1 author wishes to know whether there is significant difference in level of experience of survey participants (*refer to* **Figure 6.10**) according to their SD. As depicted in Fig.A1, the IT practitioners level of experience (with IT, cloud services, SaaS and cloud migration) are given in column 1, in column 2 a SD indicates which area of expertise survey participant's data was collected. The screen dump depicted in Fig.A2 shows the results of the one-way test performed using the two cohorts specified above. The screen dump shows the sources of variation, the degrees of freedom (DF), sums of squares (SS) and the mean square (MS) for each variance component, the variance ratio is given by F (i.e. the test statistic), and the significance of the test is shown by the p value. In fact, if $p>0.05$, there is no significant difference between the groups. But if $p<0.05$, it can be concluded that there is significant difference. The p-value 0.000 (i.e. <0.001) in Fig.A2 is below α (i.e. 0.05) suggests the result is statistically significant. This means author can generalise, from an IT practitioner's perspectives, that experience level with IT services, cloud computing, cloud migration and adoption of cloud-based SaaS services are related in larger population of enterprise decision-makers.

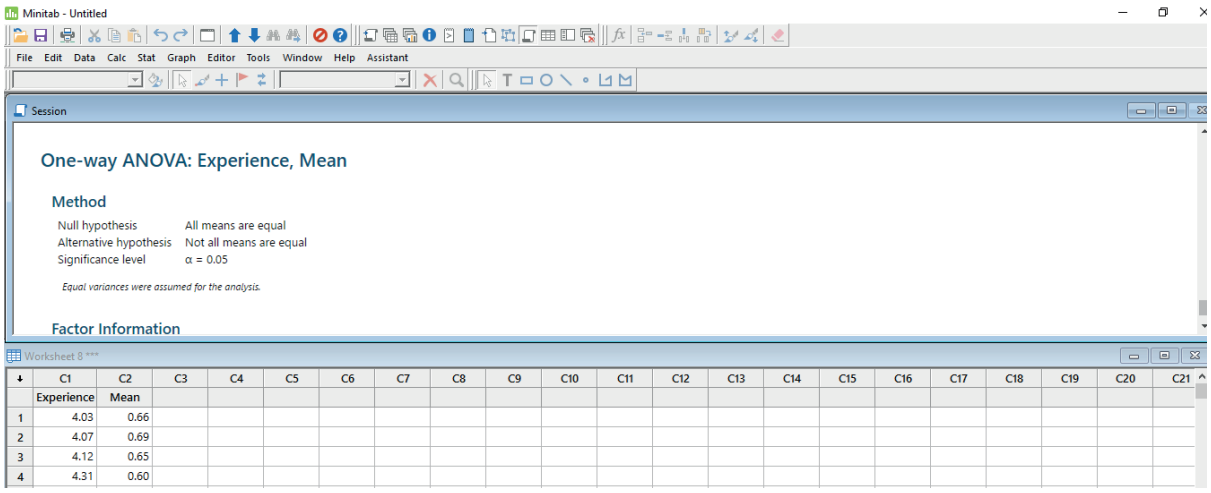


Fig. A1. Worksheet showing IT practitioners experience level (c1) from 4 different areas of expertise and their corresponding standard deviation (c2)

One-way ANOVA: Experience, Mean

Method

Null hypothesis	All means are equal
Alternative hypothesis	Not all means are equal
Significance level	α = 0.05

Equal variances were assumed for the analysis.

Factor Information

Factor	Levels	Values
Factor	2	Experience, Mean

Analysis of Variance

Source	DF	Adj SS	Adj MS	F-Value	P-Value
Factor	1	24.2556	24.2556	2894.75	0.000
Error	6	0.0503	0.0084		
Total	7	24.3059			

Model Summary

S	R-sq	R-sq(adj)	R-sq(pred)
0.0915378	99.79%	99.76%	99.63%

Means

Factor	N	Mean	StDev	95% CI
Experience	4	4.1325	0.1239	(4.0205, 4.2445)
Mean	4	0.6500	0.0374	(0.5380, 0.7620)

Pooled StDev = 0.0915378

Tukey Pairwise Comparisons

Grouping Information Using the Tukey Method and 95% Confidence

Factor	N	Mean	Grouping
Experience	4	4.1325	A
Mean	4	0.6500	B

Means that do not share a letter are significantly different.

Fig. A2. One-way Test Result for **Figure 6.10**

1.Annex_7 One-way ANOVA Test for **Figure 6.11**

Method

Null hypothesis	All means are equal
Alternative hypothesis	Not all means are equal
Significance level	α = 0.05

Equal variances were assumed for the analysis.

Factor Information

Factor	Levels	Values
SD	4	0.13, 0.23, 0.29, 0.31

Analysis of Variance

Source	DF	Adj SS	Adj MS	F-Value	P-Value
SD	3	8.569	2.856	0.66	0.648
Error	2	8.614	4.307		
Total	5	17.183			

Tukey Pairwise Comparisons

Grouping Information Using the Tukey Method and 95% Confidence

SD	N	Mean	Grouping
0.31	1	5.960	A
0.13	3	3.34	A
0.23	1	3.000	A
0.29	1	2.020	A

Means that do not share a letter are significantly different.

To interpret the ANOVA test result for **Figure 6.11**, it is important to understand that the decision-making process for a hypothesis test is based on the p-value (*see yellow highlight in table*), which indicates the probability of falsely rejecting the null hypothesis (as stated earlier in the firstt paragraph of annex_7) when it is true. In other words, if the p-value is less than or equal to a predetermined significance level (denoted by α or alpha), then one can reject the null hypothesis and claim support for the alternative hypothesis. But, if the p-value is greater than α (*see green highlight*), then one can fail to reject the null hypothesis and cannot claim support for the alternative hypothesis. Thus, with an α of 0.05, the p-value (0.648) in the Analysis of Variance table provides enough evidence to conclude that the sequence of steps within the framework is logical (as further supported with **Figure 6.12**), and the data is reasonably normal with no significant difference between the group of respondents who rated it. Please note, for clarity and brevity, due to page limitation the same analogy in the above analysis applies to every other component of the framework that is being evaluated and reported in this appendix.

2.Annex_7 One-way ANOVA Test for **Figure 6.13**

Method

Null hypothesis	All means are equal
Alternative hypothesis	Not all means are equal
Significance level	α = 0.05

Equal variances were assumed for the analysis.

Factor Information

Factor	Levels	Values
SD	4	0.71, 0.86, 0.93, 0.98

Analysis of Variance

Source	DF	Adj SS	Adj MS	F-Value	P-Value
SD	3	0.02942	0.009806	0.84	0.583
Error	2	0.02327	0.011633		
Total	5	0.05268			

Tukey Pairwise Comparisons

Grouping Information Using the Tukey Method and 95% Confidence

SD	N	Mean	Grouping
0.71	1	4.190	A
0.98	1	4.080	A
0.86	3	4.0133	A
0.93	1	3.980	A

Means that do not share a letter are significantly different.

As shown in the ANOVA test result for **Figure 6.13**, the p-value (0.583) is greater (>) than α (0.05), thus the null hypothesis can be rejected as the data looks reasonably normal. This suggests that the participant rating for *appropriateness* of the steps within the framework is valid.

3.Annex_7 One-way ANOVA Test for **Figure 6.14**

Method

Null hypothesis	All means are equal
Alternative hypothesis	Not all means are equal
Significance level	α = 0.05

Equal variances were assumed for the analysis.

Factor Information

Factor	Levels	Values
SD	5	0.78, 0.79, 0.81, 0.88, 0.93

Analysis of Variance

Source	DF	Adj SS	Adj MS	F-Value	P-Value
SD	4	0.079833	0.019958	15.97	0.185
Error	1	0.001250	0.001250		
Total	5	0.081083			

Tukey Pairwise Comparisons

Grouping Information Using the Tukey Method and 95% Confidence

SD	N	Mean	Grouping
0.78	1	4.280	A
0.79	1	4.110	A
0.93	2	4.0350	A
0.81	1	3.970	A
0.88	1	3.920	A

Means that do not share a letter are significantly different.

As shown in the ANOVA test result for **Figure 6.14**, the p-value (0.185) is greater (>) than α (0.05), thus the null hypothesis can be rejected as the data looks reasonably normal. This further suggests that the participant rating for *importance* of the steps within the framework is valid.

4.Annex_7 One-way ANOVA Test for **Figure 6.15 & Figure 6.16**

Method

Null hypothesis	All means are equal
Alternative hypothesis	Not all means are equal
Significance level	α = 0.05

Equal variances were assumed for the analysis.

Factor Information

Factor	Levels	Values
SD	8	0.77, 0.79, 0.81, 0.85, 0.87, 0.88, 0.89, 0.91

Analysis of Variance

Source	DF	Adj SS	Adj MS	F-Value	P-Value
SD	7	0.2402	0.03432	0.25	0.931
Error	2	0.2746	0.13730		
Total	9	0.5148			

Tukey Pairwise Comparisons

Grouping Information Using the Tukey Method and 95% Confidence

SD	N	Mean	Grouping
0.88	1	4.250	A
0.89	1	3.980	A
0.87	2	3.940	A
0.91	1	3.910	A
0.79	1	3.890	A
0.81	1	3.870	A
0.85	2	3.7500	A
0.77	1	3.650	A

Means that do not share a letter are significantly different.

Note the result above is a combined comparison (between *importance* and *appropriateness*) test, to detect the difference between the means for the identified tasks in **Figure(s) 6.15** and **6.16**. With an α of 0.05, the p-value (0.931) in the Analysis of Variance table provides enough evidence to conclude that the task ratings for (importance and appropriateness) are valid, and the null (H_0) hypothesis can be rejected as the data looks reasonable.

5.Annex_7 One-way ANOVA Test for **Figure 6.17 & Figure 6.18**

Method

Null hypothesis	All means are equal
Alternative hypothesis	Not all means are equal
Significance level	α = 0.05

Equal variances were assumed for the analysis.

Factor Information

Factor	Levels	Values
SD	7	0.75, 0.77, 0.88, 0.96, 0.99, 1.01, 1.04

Analysis of Variance

Source	DF	Adj SS	Adj MS	F-Value	P-Value
SD	6	0.7276	0.1213	0.57	0.765
Error	1	0.2112	0.2112		
Total	7	0.9389			

Tukey Pairwise Comparisons

Grouping Information Using the Tukey Method and 95% Confidence

SD	N	Mean	Grouping
0.88	1	4.080	A
1.01	1	4.040	A
0.77	1	3.910	A
0.96	2	3.715	A
0.99	1	3.350	A
1.04	1	3.310	A
0.75	1	3.310	A

Means that do not share a letter are significantly different.

As shown in the Analysis of Variance table for **Figure 6.17** and **Figure 6.18**, with an α of 0.05 the p-value (0.765) is greater (>) than α (0.05), thus the null hypothesis can be rejected as there is no significant difference between the group of participants who rated the tasks in step 2.

6.Annex_7 One-way ANOVA Test for **Figure 6.19 & Figure 6.20**

Method

Null hypothesis	All means are equal
Alternative hypothesis	Not all means are equal
Significance level	α = 0.05

Equal variances were assumed for the analysis.

Factor Information

Factor	Levels	Values
SD	6	0.80, 0.91, 0.92, 0.93, 0.97, 1.02

Analysis of Variance

Source	DF	Adj SS	Adj MS	F-Value	P-Value
SD	5	0.6127	0.12254	1.91	0.276
Error	4	0.2571	0.06428		
Total	9	0.8698			

Tukey Pairwise Comparisons

Grouping Information Using the Tukey Method and 95% Confidence

SD	N	Mean	Grouping
0.91	1	4.120	A
0.92	2	3.825	A
0.80	1	3.760	A
1.02	2	3.4850	A
0.97	3	3.4500	A
0.93	1	3.250	A

Means that do not share a letter are significantly different.

Again, the null (H_0) hypothesis can be rejected in this case since with an α of 0.05, the p-value (0.276), critical value of (1.91) in the Analysis of Variance table provides enough evidence to conclude that the task ratings for step 3 are valid, and there is no significant difference between the group of participants who rated it.

7.Annex_7 One-way ANOVA Test for **Figure 6.21 & Figure 6.22**

Method

Null hypothesis	All means are equal
Alternative hypothesis	Not all means are equal
Significance level	α = 0.05

Equal variances were assumed for the analysis.

Factor Information

Factor	Levels	Values
SD	7	0.84, 0.86, 0.90, 0.91, 0.95, 0.99, 1.04

Analysis of Variance

Source	DF	Adj SS	Adj MS	F-Value	P-Value
SD	6	0.3107	0.05178	0.37	0.849
Error	1	0.1404	0.14045		
Total	7	0.4512			

Tukey Pairwise Comparisons

Grouping Information Using the Tukey Method and 95% Confidence

SD	N	Mean	Grouping
0.86	1	4.190	A
0.95	1	4.070	A
1.04	1	4.040	A
0.84	2	3.875	A
0.99	1	3.680	A
0.90	1	3.680	A
0.91	1	3.610	A

Means that do not share a letter are significantly different.

To interpret the ANOVA test result for **Figure 6.20 and Figure 6.21**, with an α of 0.05, the p-value (0.849), critical value of (0.37) in the Analysis of Variance table provides enough evidence to conclude that the task ratings for step 4 is valid, hence the null (H_0) hypothesis can be rejected also as there is no significant statistical difference between study participant group.

8.Annex_7 One-way ANOVA Test for **Figure 6.23 & Figure 6.24**

Method

Null hypothesis	All means are equal
Alternative hypothesis	Not all means are equal
Significance level	α = 0.05

Equal variances were assumed for the analysis.

Factor Information

Factor	Levels	Values
SD	6	0.81, 0.86, 0.88, 0.89, 0.92, 0.93

Analysis of Variance

Source	DF	Adj SS	Adj MS	F-Value	P-Value
SD	5	0.1905	0.03810	0.70	0.652
Error	4	0.2172	0.05429		
Total	9	0.4076			

Tukey Pairwise Comparisons

Grouping Information Using the Tukey Method and 95% Confidence

SD	N	Mean	Grouping
0.89	1	4.020	A
0.93	2	3.900	A
0.88	2	3.785	A
0.86	2	3.765	A
0.81	1	3.730	A
0.92	2	3.5550	A

Means that do not share a letter are significantly different.

As shown in the Analysis of Variance table for **Figure 6.23** and **Figure 6.24**, with an α of 0.05 and critical f-value of (0.70), the p-value (0.652) is greater (>) than α (0.05), thus the null hypothesis can be rejected as there is no significant difference between the group of participants who rated the tasks in step 5.

9.Annex_7 One-way ANOVA Test for **Figure 6.25 & Figure 6.26**

Method

Null hypothesis	All means are equal
Alternative hypothesis	Not all means are equal
Significance level	α = 0.05

Equal variances were assumed for the analysis.

Factor Information

Factor	Levels	Values
SD	8	0.80, 0.83, 0.85, 0.87, 0.90, 0.95, 0.96, 1.00

Analysis of Variance

Source	DF	Adj SS	Adj MS	F-Value	P-Value
SD	7	0.941360	0.134480	63.28	0.016
Error	2	0.004250	0.002125		
Total	9	0.945610			

Tukey Pairwise Comparisons

Grouping Information Using the Tukey Method and 95% Confidence

SD	N	Mean	Grouping		
0.80	1	4.270	A		
0.87	1	4.130	A	B	
1.00	2	4.0300	A	B	
0.90	1	3.830	A	B	C
0.83	1	3.730	A	B	C
0.85	1	3.660		B	C
0.95	1	3.580		B	C
0.96	2	3.3350			C

Means that do not share a letter are significantly different.

To assess the null hypothesis, author compares the p-value to the significance level to determine whether any of the differences between the means for tasks in step 6 are statistically significant. With an α of 0.05, the p-value (0.016) < α in the Analysis of Variance table provides enough evidence to conclude that the difference between some of the means are statistically significant because not all the participant means are equal, hence the null hypothesis can be rejected as the differences are not

practically significant (*see grouping table above*). In these results, SD 0.96 and 0.80 do not share a grouping letter, which indicates that SD 0.96 has a significantly higher mean than SD 0.80. Moreover, the 95% confidence interval level for the difference between the means all include zero (0), which further indicates that all the means are not statistically significant.