Computer and Information Science; Vol. 10, No. 3; 2017
ISSN 1913-8989 E-ISSN 1913-8997
Published by Canadian Center of Science and Education

A Holistic Decision Framework to Avoid Vendor Lock-in for Cloud SaaS Migration

Justice Opara-Martins[1], Reza Sahandi[1] & Feng Tian[1]

[1] Faculty of Science and Technology, Computing and Informatics Research Centre, Bournemouth University, United Kingdom

Correspondence: Faculty of Science and Technology, Computing and Informatics Research Centre, Bournemouth University, Dorset, BH12 5BB, United Kingdom. Tel: 44-0-1202-961326. ORCHID: orcid.org/0000-0003-0639-5325. E-mail: joparamartins@bournemouth.ac.uk

Received: April 25, 2017 Accepted: June 10, 2017 Online Published: July 30, 2017

doi:10.5539/cis.v10n3p29 URL: http://doi.org/10.5539/cis.v10n3p29

Abstract

Cloud computing offers an innovative business model to enterprise for IT services consumption and delivery. Software as a Service (SaaS) is one of the cloud offerings that attract organisations as a potential solution in reducing their IT cost. However, the vast diversity among the available cloud SaaS services makes it difficult for customers to decide whose vendor services to use or even to determine a valid basis for their selections. Moreover, this variety of cloud SaaS services has led to proprietary architectures and technologies being used by cloud vendors, increasing the risk of vendor lock-in for customers. Therefore, when enterprises interact with SaaS providers within the purview of the current cloud marketplace, they often encounter significant lock-in challenges to migrating and interconnecting cloud. Hence, the complexity and variety of cloud SaaS 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 investigation has been carried out to provide a comprehensive decision framework to support enterprises on how to avoid lock-in risks when selecting and implementing cloud-based 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 minimising potential switching cost for enterprises by resolving integration issues with existing IT infrastructures. This paper proposes a holistic 6-step decision framework that enables an enterprise to assess its current IT landscape for potential SaaS replacement, and provides effective strategies to mitigate vendor lock-in risks in cloud (SaaS) migration. The 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.

Keywords: cloud computing, cloud SaaS migration, cloud-to-cloud migration, legacy-to-cloud replacement, decision framework, SaaS lock-in, vendor lock-in

1. Introduction

Advances in cloud computing research have in recent years resulted in a growing interest for migration towards the cloud environment (Opara-Martins et al. 2016). The migration to a cloud computing environment has started in earnest with the complete spectrum of businesses, from large multinational enterprises to smaller organisations, moving their IT services to cloud computing platforms (Conway & Curry, 2012). Benefits such as cost reduction, reduced maintenance overheads and flexibility in computation provide a powerful motivation for an organisation to migrate into cloud. In effect, companies are now quickly becoming reluctant to purchase more in-house hardware and software, even for business functions. Instead, small and large firms are considering adopting cloud computing services as a strategic decision with new technology and business collaboration (Gutierrez et al. 2015). Enterprise cloud Software-as-a-Service (SaaS) usage level is proliferating across categories as organisations see benefits such as IT cost saving, business agility, rapid time-to-market (value), and pay-as-you-go pricing models. The benefits of cloud computing (specifically for SaaS) over in-house development are clearly articulated and well known (Vohradsky, 2012). Nonetheless, IT cost saving has

essentially always been a major incentive within enterprises migrating to cloud-based SaaS models (Tan et al. 2013). Application rationalisation (a critical component of business transformation) is, for instance, one way to detangle this issue. In other words, the application rationalization as an enterprise-wide activity has been performed to bring down cost for operating and managing applications (Settu & Raj, 2013). SaaS is one potentially viable cloud computing service delivery option for adding to the cost saving initiatives when the rationalised applications are migrated to the cloud. However, a consensus on the main risks and challenges to SaaS is more difficult to achieve because the sourcing strategy for cloud-based SaaS offerings is often an afterthought for enterprises. Recent research study and reports confirm the aforesaid (Opara-Martins et al. 2016). For example, the typical business-led, try-and-buy purchasing patterns for cloud SaaS products have left companies (small or large) with multiple siloed instances of cloud SaaS solutions, weak integration with enterprise ICT systems and strategy, uncontrolled costs, shadow IT, and new proprietary lock-in risks to the enterprise (Herbert, 2016). Thus, the risk profile for cloud migration itself is in a state of flux, as existing offerings are maturing and new offerings are emerging. Moreover, despite initial positive results as per cost savings etc., it is challenging in theory and practice to find an appropriate provider matching the individual requirements of a company. Furthermore, the numbers of new entrants as well as non-transparent service offers, which sometimes differ significantly, make it difficult to migrate into the cloud. This difficulty, known as "proprietary, provider, or vendor lock-in" is usually the result of proprietary technologies that are incompatible with those of competitors. The vendor lock-in problem is discussed extensively and is an important research topic in many companies and international research activity e.g. Open Grid Forum (OGF) (Cattedu & Hogben, 2009; Armbrust et al. 2009). Consequently, the customer is confronted with the situation to select an appropriate provider to realize his/her specific business requirements mostly based on the existence of differentiated hardware, architectures, infrastructure, and technology used by cloud providers.

Over the last couple of years, a plethora of research efforts (Krutz & Vines 2010; Hu et al. 2011; Zhang et al. 2010; Jadeja & Modi, 2012) have been written containing SaaS risks, and specific guidance to be consulted when considering adopting cloud computing services in the enterprise (Janssen & Joha, 2011). Most focus on interoperability and portability constraints but narrow across the breadth of the broader problem of vendor lock-in where a comprehensive framework for assessment is needed to successfully manage SaaS migration projects within enterprises. This is particularly important in the context of the current cloud market place where a lot of divergent SaaS offerings with varying capabilities, system configurations, and vendor-specific restrictions (Kolb & Wirtz, 2014) are offered to customers. For cloud SaaS vendors, this differentiation is one integral part to attain and retain their market share in the face of market pressure, but for the customers this inevitably leads to proprietary lock-in risks (Bitzer, 2004; Durkee, 2010). In such a scenario, the change to a different SaaS vendor leads to significant additional migration costs (Hajjat et al. 2010; Sun & Li, 2013). So, while cloud computing may offer significant benefits, there are numerous challenges to successfully deliver cloud-based SaaS services (Vohradsky, 2012). For this reason, it becomes important to balance the benefits and advantages of cloud SaaS services against the challenges and risks. Especially, the risks concerning vendor lock-in and related challenges with switching SaaS providers and/or services are vital, and require consideration prior to a cloud deployment or migration. Our objective in this paper is to address the potential risks of lock-in affecting SaaS migration. Generally, the vendor lock-in problem is often caused by cloud computing SaaS provider's use of unique and proprietary user interfaces, application programming interfaces (APIs) and databases. Both the lock-in risks and switching difficulties need to be understood and managed before we attempt to take advantage of what cloud computing SaaS models offer.

In the light of these lock-in risks and challenges, the underpinning argument presented within this paper is that a cloud service customer's (i.e. enterprises) capability to easily switch between SaaS vendors/services without the risk of vendor lock-in is important for its decision-making regarding SaaS adoption. In other words, high switching costs or other control points such as proprietary technology integrations, data, application and contract lock-in risks make the prospect of finding an alternative SaaS vendor or technology economically unjustifiable (Polikaitis, 2015). So, if the cost to replace a SaaS vendor far outweighs the benefits, the enterprise is said to be locked into the vendor and/or technology. Therefore, to efficiently come to the correct decision about cloud SaaS migration with respect to business needs, an organisation should be able to objectively consider the aggregated risks of cloud adoption as determined by (Khajeh-HOsseini et al. 2011). Moreover, a recent review study on cloud migration research conducted by (Jamshidi et al. 2013) emphasises the necessity of a comprehensive migration framework to support an organisation through the migration decision. Such a framework should support organisations in undertaking their SaaS migration decision (to avoid vendor lock-in risks) by analysing requirements, feasibility and migration strategies, along with the execution, evaluation and cost cutting concerns on the move. To fill this gap, this paper presents a step-by-step decision framework for cloud SaaS migration

which considers a much wider range of decision steps for avoiding vendor lock-in risks, and identifies several important activities and tasks from each of them. The proposed framework is based on a sequential (step-by-step) process aiming at supporting enterprises and cloud service customers (i.e. developers, ISVs, and end-users) in making informed cloud SaaS selection and migration decisions. This framework looks to help provide a simpler, informed decision making process that is applicable to any size of organisation, and both those for whom the cloud may or may not be the best decision.

To this end, the rest of the paper is structured as follows: Section 2 presents an overview of SaaS lock-in risks, research questions and an enterprise use case scenario that motivates this study. In Section 3 we review current cloud computing migration approaches, and architectural options for enabling cloud migration. Moreover, we explore core challenges associated with switching cloud SaaS vendors/services, and review current efforts in terms of decision frameworks and tools for supporting cloud migrations. Section 4 illustrates the design process of our proposed framework as well as steps involved in each phase. In section 5, we present our proposed model that provides an overall framework for the core concepts and strategies to avoid vendor lock-in risks when adopting and migrating to cloud-based SaaS solutions. Section 6 concludes this paper.

2. Motivating Scenario

This section presents a cloud computing migration scenario chosen and adapted to specifically lay emphasis on the challenges fraught with complex enterprise cloud SaaS migration decisions, as well as to heighten the importance and need to avoid the vendor lock-in problem. The aim is to provide a high-level enterprise cloud SaaS usage scenario that is sufficiently complex for capturing real lock-in problems and sufficiently straightforward for proposing and validating research solutions. The scenario promotes portability and interoperability when migrating from one cloud SaaS vendors/services to another or back so that the switching of a cloud-based SaaS solution can occur smoothly, cost-efficiently, and securely. In our scenario, the cloud is presented as an innovation platform, for the use case of moving enterprise business data (and application components) from and between cloud SaaS vendors, or retrieving the data in case of service provider failure. The scenario addresses the lock-in issues of cloud service consumers (i.e. enterprises) who needs to switch cloud SaaS vendors/services, retrieve its own data in case that its cloud service provider cannot provide the service for a reason that can be dealt with by a disaster recovery plan (e.g. natural disaster, legal obligations etc.) or may be hard to deal with at all (e.g. bankruptcy or provider acquisition). For example, the acquisition of the cloud SaaS provider can increase the likelihood of a strategic shift for enterprises, and may put non-binding agreements at risk (e.g. software investments, non-contractual security controls) – thereby making it impossible to comply with security requirements (ENISA, 2010). The final impact of such a situation could also be damaging for crucial enterprise assets such as the organisations reputation, customer trust, employee loyalty and experience. A list of questions has been formulated to further clarify and describe our chosen scenario. Research questions to illustrate the given enterprise SaaS migration scenario are listed below:

- How to retrieve all the enterprise data held by the initial cloud SaaS vendor and move the data to the enterprises own systems (either on-site or to a designated vendor)?
- How can the enterprise smoothly move its data residing at the source SaaS product from the current cloud vendor to the target SaaS solution?
- What will happen to the enterprise data when the cloud SaaS service is no longer available and/or terminated?
- How to retrieve the data when the cloud SaaS solution becomes unavailable or perhaps vendor has gone bankrupt?

Across the exemplar use case questions presented above, the motive for the data transfer may be different, but the underlying principles, challenges, requirements for migration are quite similar (as described later in Section 3.4). For instance, a basic prerequisite in our scenario is that the requirements for data portability should be fulfilled, between the cloud SaaS vendor and enterprise (i.e. consumer), and between the old and the new cloud SaaS vendor, respectively. The level of complexity (in terms of migration decisions) in this scenario will obviously depend on the type of data (and application component) that is subject to migration. Data transfer of critical and sensitive information will obviously require more attention and most likely more work than the migration of low value and non-critical data. Thus, when planning for data migration in a SaaS enterprise usage context, it is crucial that existing data classification (e.g. criticality) and data categorisations models be used as valuable reference points for assessing the SaaS product and subsequent activities needed for the data transfer. The data classification will probably determine the level of additional measures that might be considered as contingency measures to prevent data loss in this scenario. Further, in this scenario, the definition of the cloud

SLA is critical. These might include continuous data back-up to the on-site IT environment of the cloud service consumer, back-up of the consumer's data to a secondary cloud SaaS vendor and more. Therefore, to meet the various request of enterprise cloud SaaS consumers, a few individual capabilities of the cloud SaaS service should co-exist and the related obligations and activities should be mutually agreed upon, captured in a cloud service level agreement (SLA) or corresponding agreement (contract) set up between the consumer and the cloud SaaS vendors. Furthermore, it is also critical to understand the implications of any legislation or regulation in effect, that is relevant for the data migration. This is particularly significant if the enterprise data, in question, is to be moved over geographies with different overarching legislation, e.g. from any member states within the European Union (EU), to a country outside of the EU (e.g. United Kingdom).

3. Background and Related Work

3.1 Migration to SaaS Clouds – An Overview

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. The delivery of a software "as a service" implies that the base of the resources is off-premises relative to the consumer – in other words, the term "as a service" implies that it is off-premises. SaaS involves off-premise resources (typically, business applications) offered in a one-to-many manner – that is, multiple organisations using the same application but in manner that each user organisation experiences as if it were the only entity using the application. The one-to-many model of software delivery can be implemented through multi-tenancy or isolated tenancy. Multi-tenancy implies elasticity, while isolate tenancy allocates fixed isolated resources to each user organisation. In cloud computing, SaaS migration is the process of switching from one cloud vendors operating environment to another SaaS vendor that in most cases is better (Zhao & Zhou, 2014). Computing off-premises is a long-standing enterprise practice (Natis et al. 2008). The term off-premise in SaaS context indicates the computing service (including the application and the data) resides on hardware that the service consumer does not own. In the off-premise IT scenario, there are always two parties involved: the provider of the resources (i.e. vendor) and the one that rents them (i.e. the consumer organisation). We will use these terms in this section to refer to these two roles throughout this paper.

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 & Mahowald, 2015). The adoption 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 & Wagle, 2007). Thus, migration to SaaS clouds has become an attractive proposition to cloud computing consumers. For example, enterprise cloud SaaS consumers and end-users are interested in exploiting the benefits of reducing software and computing-related investment and operating costs, while developers on the other hand may be interested in creating and opening new business models and sources of revenues and profits. In this example, the delivery and consumption of cloud SaaS services may be cheaper for either party involved than an in-house system – i.e., since consumers particularly expect to save on support and upgrade costs, IT infrastructure, personnel and implementation. However, besides maintainability issues, on-premise legacy systems are still crucial within certain organisations as they support core enterprise business processes and applications that cannot be easily replaced (Jamshidi et al. 2013).

Traditional software application users will usually manage such risks by customizing the software product they build or buy, to ensure that the application meets the business requirements accordingly. In the SaaS context, vendors often create application configuration with pre-defined and adjusted configuration scope to address the known circumstances. The main difference between customisation and configuration in this case, is that the latter does not involve source code changes whereas customisation does (Singh & Sanaman, 2012). While some configuration can be setup with predefined parameters to change software functionality that maybe possible in SaaS solutions, however beyond such cost-effective predefined range of functionality, cloud-based SaaS service(s) is not intended to offer customised solutions.

Another differentiating attribute for cloud-based services with traditional software is that, SaaS involves the payment of periodic fees instead of a large initial investment. Hence, cloud service consumers will retain the option to switch to another SaaS vendor if they believe it is appropriate to do so. However, switching between SaaS vendors and/or services in the current cloud marketplace is not free, due to the business relationship

between parties involved. Thus, switching from a source SaaS vendor solution to a target SaaS vendor will require the cloud service consumer to experience data transfer and recovery costs, which are significant switching costs the enterprise must consider when making decisions to adopt and migrate to cloud-based SaaS service. Moreover, if the SaaS vendor does not provide a mechanism to extract the data provided by the cloud service consumer during the use of the SaaS application, the consumer may find itself in a similar position in time prior to its relationship with the incumbent SaaS vendor (Stucke, 2013). Furthermore, the ownership of the data necessary to operate the SaaS application in the cloud may create another vendor control point if not clearly addressed in the cloud service contract agreement. The question of what the cloud service consumer can do with the data outside the context of SaaS may involve legal issues and opposing legal opinions. Potential impact of these issues on enterprises involved in a cloud computing system accelerate the need to further investigate and identify core challenges to switching between SaaS vendors before procuring and selecting cloud-based ICT services. In the next section, we discuss these challenges in detail as they represent shared concerns that need to address (e.g. interoperability, portability, security requirements and effective strategies for their implementation) when migrating to or deploying a cloud computing SaaS system.

3.2 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 paper.

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 & 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 (Polikaitis, 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 (*sub-section C*)**.**

3.3 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 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. 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.

3.4 Challenges with Switching between Cloud SaaS Vendors

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. 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. The following constraints and challenges have been identified with switching between cloud SaaS vendors: switching cost (Zhu &Zhou, 2012), data portability (Petcu, 2011), API propagation (Parameswaran & Chaddha, 2009) and integration issues (Opara-Martins et al. 2015a), interoperability and standards [39], security risks, contract and SLA management (Opara-Martins et al. 2015b), and legal challenges (data location constraints, data ownership rights, cloud in/exit issues, legal jurisdiction and compliance etc.). They have been further grouped hierarchically into three main challenge areas of SaaS migration, and analysed in detail below. Figure 1 illustrates the categorisation of challenges associated with changing cloud SaaS vendors across each of these three main areas. These challenges represent shared concerns that need to be addressed prior to SaaS adoption, or switching between cloud SaaS service and vendors.

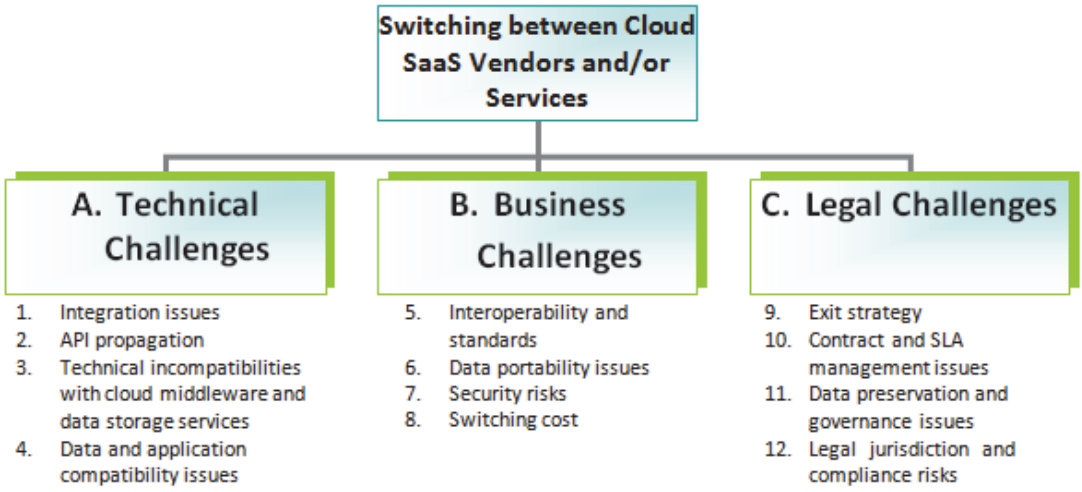

Figure 1. Key Categories of Issues Identified with Cloud SaaS Migrations

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 in Figure 1 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. 2012). 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. 2015a). 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 the work of (Opara-Martins et al. 2015a).

- *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 (Parameswaran & Chaddha, 2009) problem. 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). To classify portability as a business challenge there are three recommend three issues that need to be resolved: i.e. (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 (Cabral, 2012; Farrel & Klemperer, 2007). Whereas others have disagreed, they argue that switching costs reduce market competitiveness, raise prices, and support customer lock-in (Beggs & Klemperer, 1992; Farrel & Shapiro, 1988; Klemperer, 1987; Klemperer, 1987; Klemperer, 1989). 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 & 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. In (Gartner Research Report, 2013), 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. 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, 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 & 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.

3.5 Decision Frameworks and Tools for Supporting Cloud SaaS Migration in Enterprises

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 lock-in risks and insufficient due diligence were among the top threats in cloud computing (Dutta et al. 2013; Baldwin et al. 2013). Cloud computing adoption decisions are challenging due to various concerns such as cost, confidentiality and control (Khajeh-Hosseini et al. 2012). Organisations that adopt, or migrate to, cloud computing services often do not understand the resulting risks (Dutta et al. 2013). 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 (Andrikopolous et al. 2013). 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. 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 (Whaiduzzaman 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 & Mulik, 2009). Besides, 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 migration process will result in noticeable changes to how systems are developed and supported (Khajeh-Hosseini et al. 2010).

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 & Pingali, 2011; Bibi et al. 2010; Frey & Hasselbring, 2011; Zardari & 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 & Babar, 2011; Khajeh-Hosseini et al. 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 & Ajila, 2013), or the costs when deploying the application (Sulieman et al. 2012; Liew & Su, 2012). 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 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; Chappell, 2009), while IT consultancies on the other hand are offering frameworks (Ward et al. 2010; Alonso et al. 2013; Tan et al. 2013; Donnellan et al. 2011; Garg et al. 2013; Catteddu & hogben, 2009) and assessment tools (Boruff, 2009; Accenture, 2009; Herbert, 2013), 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 (Andrikopoulos et al. 2013) 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. 2013; Tan et al. 2013) 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. In the next section, we propose a novel decision framework (with strategic guidelines) to mitigate lock-in risks in cloud SaaS migration for enterprise adoption.

4. A Holistic Decision Framework to Mitigate Vendor Lock-in Risks in Cloud SaaS Migration

This section introduces our proposed decision framework, designed for use by enterprises that are already consuming or considering adopting cloud-based SaaS offerings. Our decision framework can be used by 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. The development of the decision framework followed an approach used to develop the maturity model for sustainable ICT in (Donnellan et al. 2011), and was undertaken using a design process with defined review stages and development activities that were based on the Design Science Research (DSR) guidelines advocated by Hevner et al. (2004). Our work was initially targeted at the vendor lock-in challenges of cloud SaaS services adoption and migration. Further, this led us to leverage the work by Cullen et al in (Cullen et al. 2009), into the management and mitigation of cloud computing vendor lock-in risks using a decision framework. Cullen's life cycle has been adapted and the resulting life cycle has been applied to the problems of managing elements of vendor lock-in risks in cloud SaaS migration. We have examined the requirements of cloud software (SaaS) application migration from two distinct viewpoints: user view, functional view, implementation view and deployment view (ITU 2014). 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.

4.1 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. Epistemologically, the overall study design consists of two distinct phases as further explained in our most recent work (Opara-Martins et al. 2016). 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. From this perspective, the use of interview was appropriate research method, as it enabled depth, nuance and complexity in data to be captured (Carcary, 2009; Mason, 2002). Five participants from different industry sectors and organisations 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. After the pilot interview phase, a questionnaire was designed for a survey. The main issues raised at the interviews were incorporated into the 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. In synthesis, both phases of the research design helped in capturing the views of key domain experts and to understand the elements of vendor lock-in and associated barriers to managing cloud SaaS migration projects (whether public, private or hybrid ones). Furthermore, relevant literature, both industry standards as well as academic materials were consulted to substantiate and support the framework development. The findings from the systematic literature review have been discussed

broadly in the works of (Opara-Martins et al. 2016; Opara-Martins et al. 2014; Opara-Martins et al. 2015a; Opara-Martins et al. 2015b). 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 below) 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 **2** 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 **2**), 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?".

4.2 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 lifecycle decision process for cloud SaaS service migration to avoid vendor lock-in risks, illustrated in Figure **3**, 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 publication. 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. The six steps and corresponding activities should be carried out per the process workflow shown in Figure 4. 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 (Jamshidi et al. 2013). The three main phases of the cloud SaaS migration process are: Phase 1 – Service Selection and Evaluation; Phase 2 – Contract and Service Provision; and Phase 3 – Service Management and Optimization.

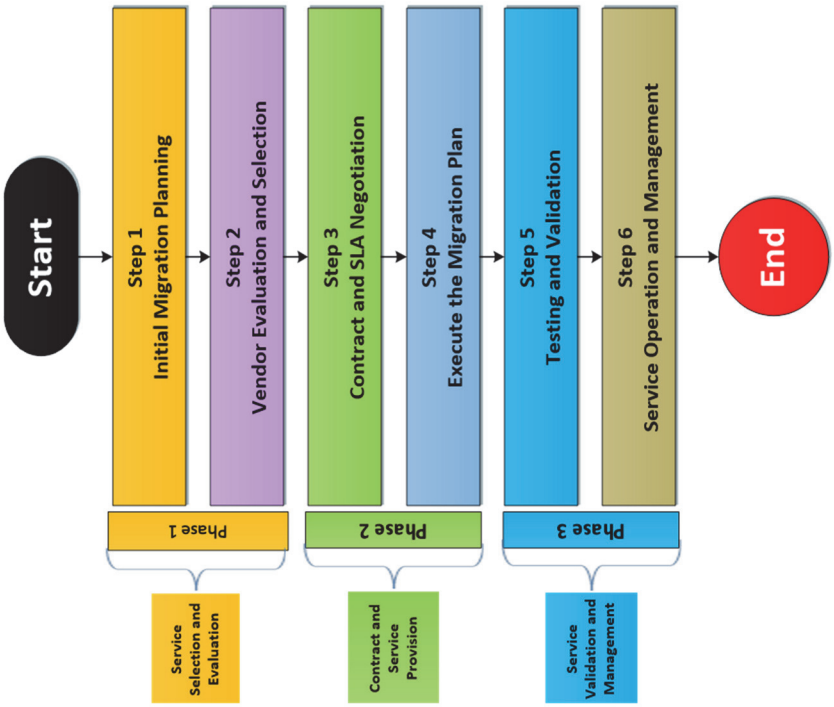

Figure 2. Cloud Decision Framework Overview

Figure 3. A Lifecycle for Managing Vendor Lock-in Risks in Cloud SaaS Migration

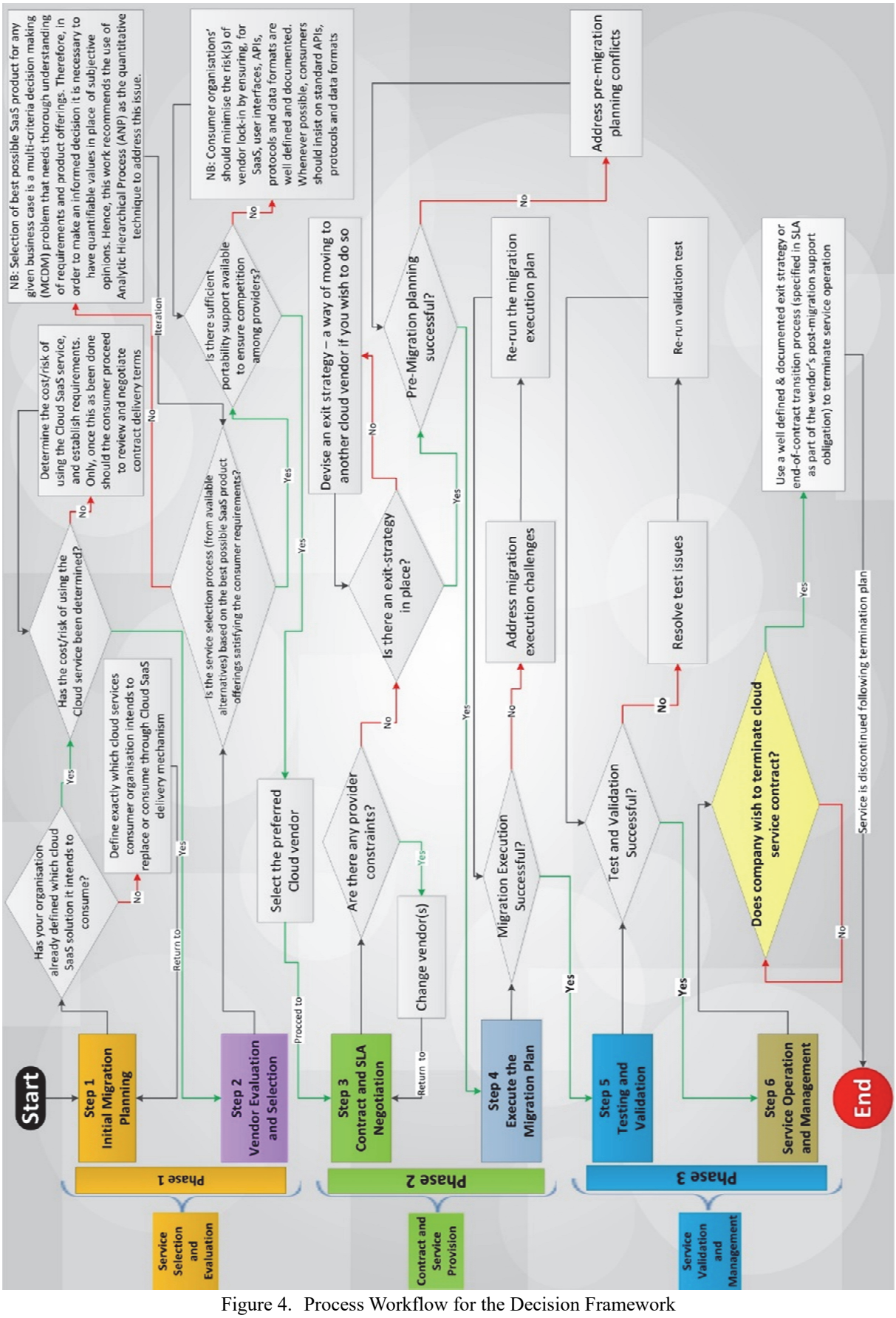

Figure 4. Process Workflow for the Decision Framework

5. Process Workflow for the Decision FrameworkThe Decision Framework Sequence

In subsequent section, we elaborate on the phases involved in our proposed framework for avoiding vendor lock-in risks in cloud SaaS migration. Each phase provides a prescriptive series of steps that cloud service consumers should take when considering 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.

5.1 Phase 1: Service Selection and Evaluation Process

Phase 1 (as depicted in Figure **5**) 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. Therefore, 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 interoperable cloud solutions. The decision steps and supporting activities involved in this phase are comprehensively discussed in our future work.

5.2 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 **6**), 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.

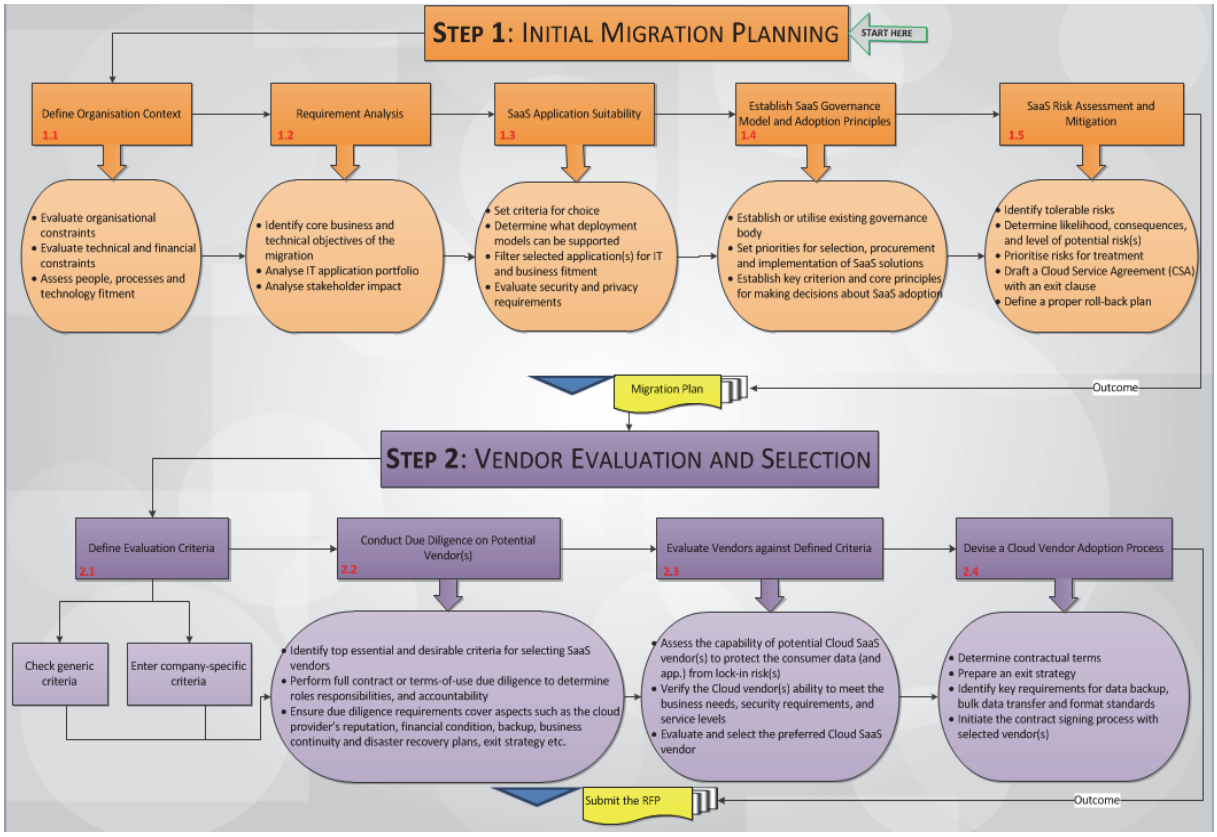

Figure 5. Key Activities and Outputs for Phase 1

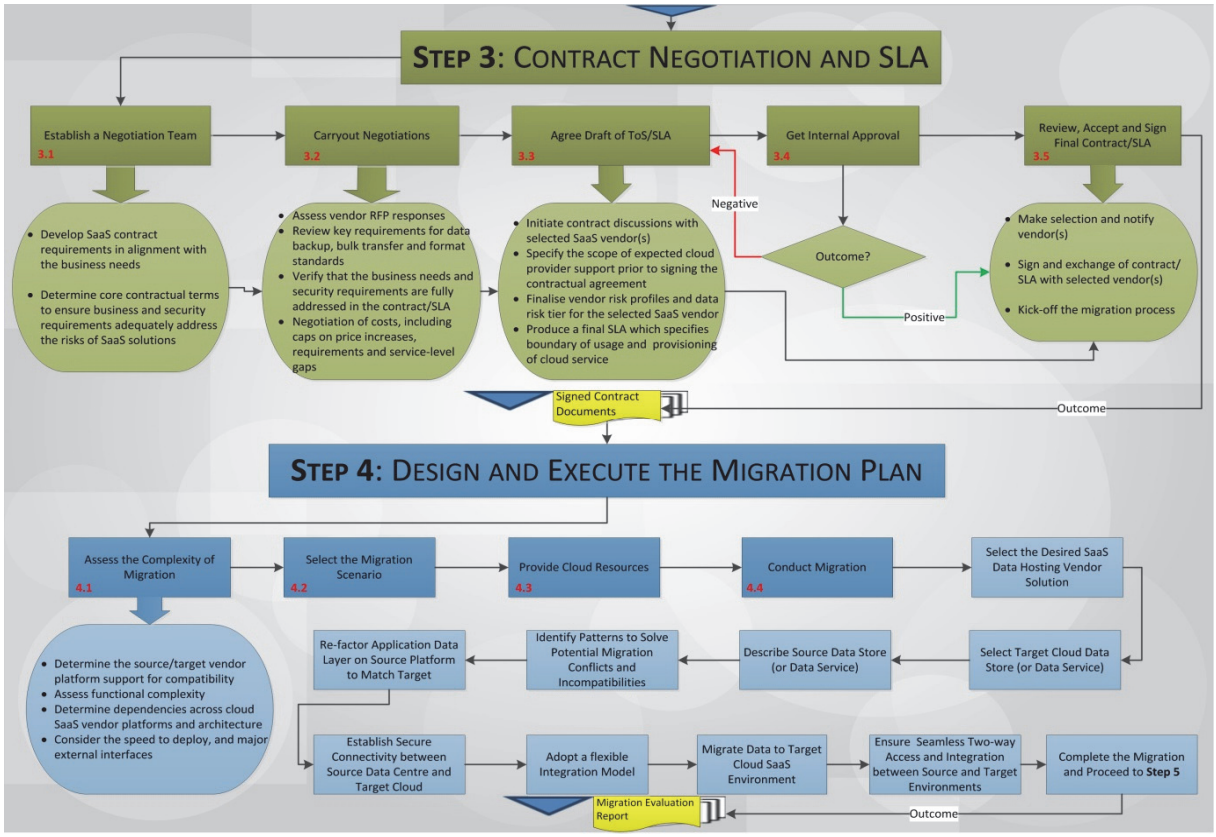

Figure 6. Contract and Service Provision Phase 2

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. For example, to ensure the migrated SaaS service continuously achieves its business objectives without any business disruption, the migration process in this phase is evaluated to appropriately address both external and internal factors to avoid vendor lock-in and improve overall business performance. Hence to effectively provision selected migrated SaaS services, enterprises must have a rethink of their business applications and services as provisioning services rather than simply contracting assets. 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.

5.3 *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 (as shown in Figure **7**) 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.

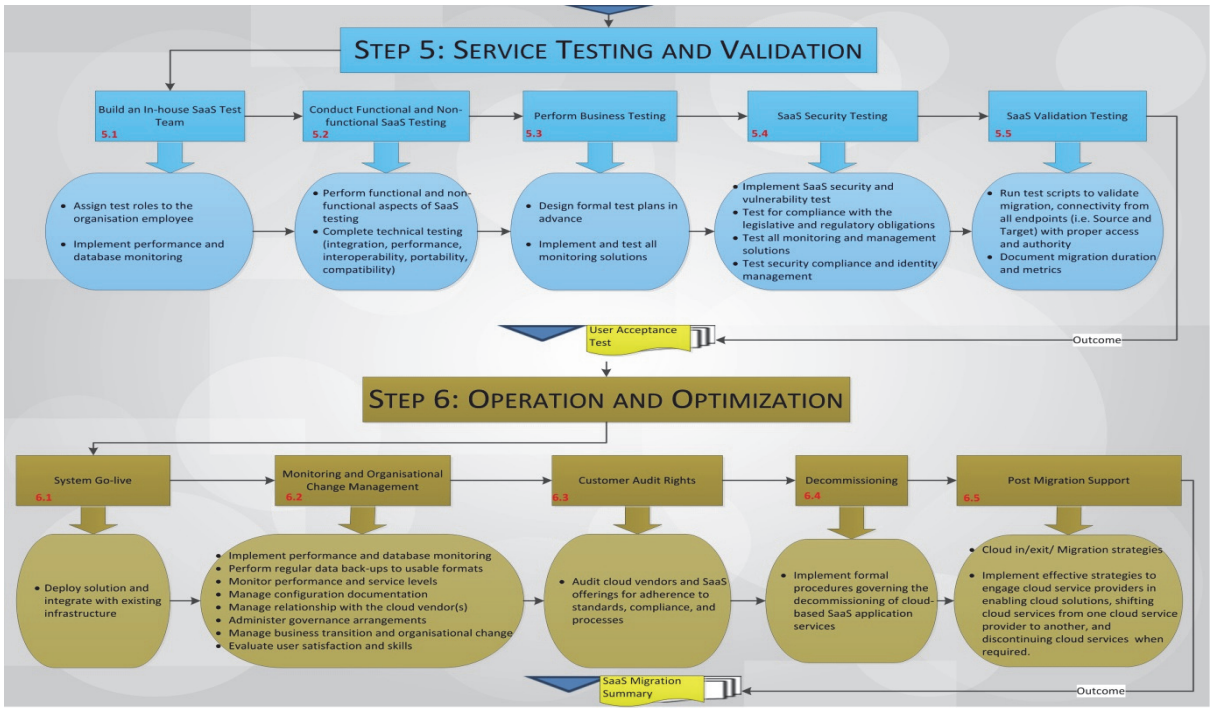

Figure 7. Service Validation and Management Phase 3

5.4 Optional Step – Service Termination or Rollback

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.

6. Conclusion

In this paper, we have shown that cloud computing is a venture with an attractive proposition to enterprises, small or large. Consequently, enterprises are rapidly utilising cloud-based SaaS services to address specific business needs. However, several challenges remain inadequately addressed and as such require scrutiny to facilitate the widespread adoption and maturity of the cloud SaaS marketplace. The discussions presented herein specifically address, from a business perspective, pertinent cloud migration issues, data privacy and security risks, and concerns about SaaS lock-in. At a higher level, this paper identifies relevant cloud SaaS migration challenges related to security, privacy, lock-in (i.e. interoperability and portability issues) as well as contractual clauses to which businesses need to exercise great attention. Being that there are many aspects to SaaS lock-in, we have also discussed issues related to exit strategy and contract termination (including data retention and destruction). This also includes the importance of retaining metadata as well as data ownership rights. Moreover, on the legal side, increasing attention is paid by businesses to cloud computing contracts and SLA, which are hitherto still framed in proprietary forms by cloud service providers. Further complexity to this proprietary form is that neither the terminology of SLAs nor the willingness to negotiate SLAs is consistent between different cloud providers. In light of these lock-in risks and challenges, the underpinning argument presented within this paper is that a cloud service customers (i.e. enterprises) capability to easily switch between SaaS vendors/services without the risk of vendor lock-in is important for its decision-making regarding SaaS adoption. So, if the cost to replace a SaaS vendor far outweighs the benefits, the enterprise is said to be locked in to the vendor and/or technology. Therefore, to efficiently come to the correct decision about cloud SaaS migration with respect to business needs, an organisation should be able to objectively consider the aggregated lock-in risks of cloud SaaS adoption.

The SaaS lock-in problem is often caused by cloud computing vendor's use of unique and proprietary user interfaces, application programming interfaces (APIs) and databases. Both the associated lock-in risks and switching difficulties need to be understood and managed before attempting to take advantage of what cloud computing SaaS models should offer. To this end, we have proposed a decision framework to support cloud SaaS migration in enterprises. The framework aims to address the core scenario questions that motivate our work. These include contractual matters which must be considered and implemented before adopting the SaaS 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. The level of formalisation between the six main steps in the framework is so distinct that each decision step has a clearly defined task that they relate to. 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. 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 in implementation with reduced effort. The corresponding framework can be used to aid cloud service consumers in terms of better understanding the lock-in risks specific to core components (or constituents) of cloud SaaS services. In turn, this will support the advancement of SaaS migration and cloud computing adoption, in general.

In future work, we plan to critically investigate how the decision to avoid vendor lock-in risks in cloud SaaS migration can be managed within each step in our proposed framework. This includes discussing how the already identified steps, supporting activities, and relationships are linked between the decisions that need to be made when switching/changing cloud SaaS vendors and/or services to avoid vendor lock-in risks. The focus is to show how our framework can be used to support cloud service consumers and enterprises aiding to determine the appropriate cloud SaaS offerings for their business needs. We also plan to evaluate our proposed framework with a wide profile of IT practitioners, cloud consultants, industry researchers and academia. To this end, we will further evaluate the overall effectiveness of the framework by performing quantitative data analysis, and thereafter report our findings in future publication.

Competing interests

The authors declare that they have no competing interests.

Authors' information

Justice Opara-Martins is a Doctoral (PhD) researcher in cloud computing at Bournemouth University where he graduated with an MSc in Wireless and Mobile Networks. He holds a BSc (Hons.) in Information and Communication Technology. He is a Fellow of the Higher Education Academy (FHEA), and a member of the British Computer Society (BCS), IBM Academic Initiative and Association for Project Managers (APM). His research interests include cloud computing, virtualization, Big Data, information management and distributed systems.

Reza Sahandi completed his PhD at Bradford University in the United Kingdom in 1978. He has been a senior academic at various Universities in the United Kingdom for many years. He is currently an Associate Professor at Bournemouth University. His research areas include multimedia and network systems, wireless remote patient monitoring and cloud computing.

Feng Tian received the PhD degree from Xi'an Jiaotong University, China. Currently he is an Associate Professor at Bournemouth University (BU), United Kingdom. He was an Assistant Professor in Nanyang Technological University in Singapore before joining BU in 2009. His current research interests include computer graphics, computer animation, augmented reality, image processing and cloud computing.

Acknowledgments

All listed authors made substantive intellectual contributions to the research and manuscript. JOM was responsible for the overall vendor lock-in research including proposing the novel holistic framework, drafting the manuscript, conducting the literature analysis and interpretation of study results. RS, FT and JOM contributed to the design of proposed framework. RS and FT participated in the critical and technical revisions of the paper including editing the final version, also helping with the details for preparing the paper to be published. RS and FT coordinated and supervised the project related to the manuscript and also gave final approval of the version to be published. All authors read and approved final manuscript.

References

Accenture. (2009). *Accenture Cloud Computing Accelerator.* Retrieved from http://www.longwoods.com/blog/wp-content/uploads/2010/07/Accenture_Technology_Labs_Cloud_Computing_Accelerator.pdf

Ahronovitz, M. et al. (2010). *Cloud Computing Use Cases - A white paper by the Cloud Computing Use Case Discussion Group.* Retrieved January 8, 2017, from http://www.cloud-council.org/Cloud_Computing_Use_Cases_Whitepaper-4_0.pdf

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

Alonso, J., Orue-Echevarria, L., Escalante, M., Gorroñogoitia, J., & Presenza, D. (2013). Cloud modernization assessment framework: Analyzing the impact of a potential migration to Cloud. In *Maintenance and Evolution of Service-Oriented and Cloud-Based Systems (MESOCA), 2013 IEEE 7th International Symposium on the* (pp. 64-73) September. IEEE

Andrikopolous, V., Binz, T., Leymann, F., & Strauch, S. (2013). How to Adapt Applications for the Cloud Environment. *Computing, 95*(6), 493-535

Andrikopoulos, V., Strauch, S., & Leymann, F. (2013). Decision Support for Application Migration to the Cloud: Challenges and Vision. In: 3rd International Conference on Cloud Computing (CLOUD 2014). IEEE

Armbrust, M., Fox, A., Griffith, R., Joseph, A. D., Katz., R. H., Konwinski, A., Lee, G., Patterson, D. A., Rabkin, A., Stoica, I., & Zaharia, M. (2009). Above the Clouds: A Berkeley View of Cloud Computing, UC Berkeley Reliable Adaptive Distributed Systems Laboratory

Baldwin, A., Pym, D., & Shiu, S. (2013). Enterprise information risk management: Dealing with cloud computing. In *Privacy and Security for Cloud Computing*, pp. 257-291. Springer London

Bankole, A., & Ajila, S. (2013). Cloud client prediction models for cloud resource provisioning in a multitier web application environment. In Proceedings of SOSE'13, March 2013, pp. 156–161

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

Bibi, S., Katsaros, D., & Bozanis, P. (2010). Application development: Fly to the clouds or stay in-house?

In *Enabling Technologies: Infrastructures for Collaborative Enterprises (WETICE), 2010 19th IEEE International Workshop on* (pp. 60-65). IEEE

Bitzer, J. (2004). Commercial versus Open Source Software: Role of Product Heterogeneity in Competition. In *Economic Systems Journal, 28*(4), 369–381

Boruff, B. (2009), Computer Sciences Corporation. Cloud Adoption Assessment: Doing Business in the Cloud. Retrieved from http://assets1.csc.com/dk/downloads/DoingBusinessInTheCloud.pdf

Burns, M. (2012). Cloud-based ERP: the risk of Vendor Lock-in. In Emerging Issues and Technologies for ERP Systems, Class of Enterprise Systems Integration, 2011-12. School of Computing and Mathematics, University of Derby, UK, pp.77 – 80

Cabral, L. (2012). Switching costs and equilibrium prices, New York University. Retrieved from https://archive.nyu.edu/jspui/bitstream/2451/31545/2/Cabral-SwitchingCostsandEquilibriumPrices_Mar2012.pdf

Carcary, M. (2009). The research audit trial–enhancing trustworthiness in qualitative inquiry. *The Electronic Journal of Business Research Methods*, *7*(1), 11-24

Catteddu, D., & Hogben, G. (2009). Cloud Computing - Benefits, risks and recommendations for information security, *European Network and Information Security Agency* (ENISA)

Cayirci, E., Garaga, A., de Oliveira, A. S., & Roudier, Y. (2016). A risk assessment model for selecting cloud service providers. *Journal of Cloud Computing*, *5*(1), 14.

Chappell, D. (2009). Windows Azure and ISVs: A Guide for Decision Makers, July 2009. Retrieved from http://download.microsoft.com/download/e/7/4/e74d55e6-d156-404f-b6c5-a53a9a4b1d42/windows%20azure%20for%20isvs%20v1%2011--chappell.pdf

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

Conway, G., & Curry, E. (2012). Managing Cloud Computing-A Life Cycle Approach. In *CLOSER* pp. 198-207

Conway, G., & Curry, E. (2013) The IVI Cloud Computing Life Cycle. *Cloud Computing and Services Science*, pp. 183-199

Cullen, S., Seddon, P., & Willcocks, L.P. (2009). Managing Outsourcing: The Life Cycle Imperative, Strategic Information Management, 4, 494 – 519

De Filippi, P., McCarthy, S. (2012). Cloud Computing: Centralization and Data Sovereignty. European Journal for Law and Technology, 3(2). Retrieved from http://ejlt.org/article/view/101/234

Donnellan, B., Sheridan, C., & Curry, E. (2011). A capability maturity framework for sustainable information and communication technology. *IT professional*, *13*(1), 33-40

Dubé, J.P., Hitsch, G.J., & Rossi, P.E. (2009). Do switching costs make markets less competitive? *Journal of marketing research*, *46*(4), 435-445

Dubey, A., & Wagle, D. (2007). Delivering software as a service, McKinsey Quart., vol. 6, pp. 1–12, Jun. (2007)

Durkee, D. (2010). Why Cloud Computing Will Never be Free. In *Communications of the ACM,* 53(4), 369–381.

Dutta, A., Peng, G. C. A., & Choudhary, A. (2013). Risks in enterprise cloud computing: the perspective of IT experts. *Journal of Computer Information Systems*, *53*(4), 39-48

ENISA. (2010). Benefits, risks and recommendations for Information Security. Retrieved from https://resilience.enisa.europa.eu/cloud-security-and-resilience/publications/cloud-computing-benefits-risks-and-recommendations-for-information-security Accessed 24 November 2016

Farrell, J., & Klemperer, P. (2007). Coordination and lock-in: Competition with switching costs and network effects. *Handbook of industrial organization*, *3*, 1967-2072.

Farrell, J., & Shapiro, C. (1988). Dynamic competition with switching costs. *The RAND Journal of Economics*, pp. 123-137

Frey, S., & 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.

Garg, S.K., Versteeg, S., & Buyya, R. (2013). A Framework for Ranking of Cloud Computing Services. *Future*

Generation Computer Systems, 29(4), 1012–1023

Gartner Research (2013). Devising a Cloud Exit Strategy: *Proper Planning Prevents Poor Performance*. Retrieved from https://www.gartner.com/doc/2397615/devising-cloud-exit-strategy-proper Accessed on 7th January 2017.

Godse, M., & Mulik, S. (2009). An approach for selecting software-as-a-service (SaaS) product. In *Cloud Computing, 2009. CLOUD'09. IEEE International Conference on* (pp. 155-158) September. IEEE.

Gutierrez, A., Boukrami, E., & Lumsden, R. (2015). Technological, Organisational and Environmental Factors Influencing Managers' Decision to Adopt Cloud Computing in the UK. *Journal of Enterprise Information Management*, *28*(6), 788-807

Hajjat, M., Sun, X., Sung, Y. W. E., Maltz, D., Rao, S., Sripanidkulchai, K., & Tawarmalani, M. (2010). Cloudward Bound: Planning for Beneficial Migration of Enterprise Applications to the Cloud. In *ACM SIGCOMM Computer Communication Review,* 40(4), 243–254.

Herbert, L. (2013). Forrester SaaS Capabilities Maturity Assessment. Forrester Research. Retrieved from http://media.cms.bmc.com/documents/Forrester_SaaS_Capabilities_Maturitity_Assessment+(2).pdf

Herbet, L. (2016). SaaS Readiness Assessment – Making SaaS Succeed In Customer-Obsessed Business Models. Retrieved from https://www.forrester.com/report/SaaS+Readiness+Assessment/-/E-RES88921

Hevner, A. R., March, S. T., Park, J., & Ram, S. (2004). Design science in information systems research. *MIS Quarterly, 28*(1), 75-105.

Hu, F., Qiu, M., Li, J., Grant, T., Taylor, D., McCaleb, S., Butler, L., & Hamner, R. (2011). A Review on Cloud Computing: Design Challenges in Architecture and Security. CIT. *Journal of Computing and Information Technology, 19*(1), 25–55

ITU, (2014). Information Technology – Cloud Computing – Reference Architecture. Retrieved from http://www.itu.int/rec/T-REC-Y.3502-201408-I

Jadeja, Y., & Modi, K. (2012). Cloud Computing-concepts, Architecture and Challenges. In *International Conference on Computing, Electronics and Electrical Technologies* (ICCEET), 877–880. IEEE.

Jamshidi, P., Ahmad, A., & Pahl, C. (2013). Cloud migration research: a systematic review. *IEEE Transactions on Cloud Computing*, *1*(2), 142-157.

Janssen, M., & Joha, A. (2011). Challenges for Adopting Cloud-based Software as a Service (SaaS) in the Public Sector. In *European Conference on Information Systems (ECIS) Proceedings, Paper 80*. Association for Information Systems (AIS) Electronic Library.

Khajeh-Hosseini, A., Greenwood, D., & 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., Greenwood, D., Smith, J. W., & Sommerville, I. (2012). The Cloud Adoption Toolkit: Supporting Cloud Adoption Decisions in the Enterprise. *Software: Practice and Experience, 42*(4), 447-465.

Khajeh-Hosseini, A., Sommerville, I., Bogaerts, J., & Teregowda, P. (2011). Decision support tools for cloud migration in the enterprise. In *Cloud Computing (CLOUD), 2011 IEEE International Conference,* pp. 541-548 IEEE.

Klemperer, P. (1987). Markets with consumer switching costs. *The Quarterly Journal of Economics*, *102*(2), 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), 405-420.

Kolb, S., & Wirtz, G. (2014), Towards Application Portability in Platform as a Service. In 2014 IEEE 8th International Symposium on *Service Oriented System Engineering* (SOSE).

Krutz, RL., & Vines, RD. (2010). Cloud Security: *A Comprehensive Guide to Secure Cloud Computing*, Wiley Publishing.

Liew, S. H., & Su, Y. Y. (2012). Cloudguide: Helping users estimate cloud deployment cost and performance for

legacy web applications. In *Cloud Computing Technology and Science (CloudCom), 2012 IEEE 4th International Conference on* (pp. 90-98) December. IEEE

Ma, D., & Kauffman, R. J. (2014). Competition between software-as-a-service vendors. *IEEE Transactions on Engineering Management*, *61*(4), 717-729.

Mason, J. (2002). *Qualitative Researching*. London, Sage Press.

McGrath, B., & Mahowald, P. R. (2015). Worldwide SaaS and Cloud Software 2015-2019 Forecast and 2014 Vendor Shares. Retrieved from https://www.idc.com/getdoc.jsp?containerId=257397

Miranda, J., Guillen, J., Murillo, J. M., & Canal, C. (2013). Assisting cloud service migration using software adaptation techniques. In *Cloud Computing (CLOUD), 2013 IEEE Sixth International Conference on* (pp. 573-580) June, IEEE

Natis, Y. V., Gall, N., Cearley, D. W., Leong, L., Desisto, R. P., Lheureux, B. J., Smith, D. M., Plummer, D. C. (2008). Cloud, SaaS, hosting and other off-premises computing models. *Retrieved March*, *1*, p.2009.

Opara-Martins, J., Sahandi, R., & Tian, F. (2015) 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. (2015). 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. (2016). Critical Analysis of Vendor Lock-in and its Impact on Cloud Computing Migration: A Business Perspective. *Journal of Cloud Computing, 5*(1), 1-18.

Opara-Martins. J., Sahandi, R., & Tian, F. (2014). 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) November. IEEE.

Parameswaran, A. V., & Chaddha, A. (2009). Cloud interoperability and standardization. *SETlabs briefings*, *7*(7), 19-26.

Petcu, D. (2011). Portability and interoperability between clouds: challenges and case study. In *European Conference on a Service-Based Internet* (pp. 62-74) October. Springer Berlin Heidelberg.

Petcu, D., Craciun, C., & Rak, M. (2011). Towards a cross platform cloud API. In *1st International Conference on Cloud Computing and Services Science,* 166-169.

Polikaitis, A. (2015). Vendor and Sourcing Management: *Maintaining Control of Vendor Relationships by Avoiding Vendor Lock-in*. IDC Opinion Report. Retrieved from http://core0.staticworld.net/assets/2016/04/19/idc-vsm-avoiding-vendor-lock-in.pdf. Accessed 12 November 2016

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., & Opara-Martins, J. (2013). Cloud computing from SME's perspective: A survey-based investigation. *Journal of Information Technology Management*, *24*(1), 1-12.

Saripalli, P., & Pingali, G. (2011). Madmac: Multiple attribute decision methodology for adoption of clouds. In *Cloud Computing (CLOUD), 2011 IEEE International Conference on* (pp. 316-323) July. IEEE.

Settu, R., & Raj, P. (2013). Cloud Application Modernization and Migration Methodology. *In Cloud Computing: Methods and Practical Approaches (Chap 12)*. Springer Publishing Company, Incorporated. Edited by Mahmood, Z. Retrieved from http://dl.acm.org/citation.cfm?id=2517809

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%20CostShin%20and%20Sudhir% 202008.pdf

Singh, M., & Sanaman, G. (2012). Open source integrated library management systems: Comparative analysis of Koha and NewGenLib. *The Electronic Library*, *30*(6), 809-832.

Stucke, M.E. (2013). Is competition always good? *Journal of antitrust Enforcement*, *1*(1), 162-197.

Suleiman, B., Sakr, S., Jeffery, R., & Liu, A. (2012). On understanding the economics and elasticity challenges

of deploying business applications on public cloud infrastructure. *Journal of Internet Services and Applications*, *3*(2), 173-193.

Sun, K., & Li, Y. (2013). Effort Estimation in Cloud Migration Process. *In 7th IEEE International Symposium on Service-Oriented System Engineering (SOSE)*, pp. 84 – 91, San Francisco, United States

Tan, C., Liu, K., Sun, L. (2013). A Design of Evaluation Method for SaaS in Cloud Computing. *Journal of Industrial Engineering and Management JIEM, 6*(1), 50–72.

Tan, C., Liu, K., Sun, L., & Spence, C. (2013). An evaluation framework for migrating application to the cloud: software as a service. In *LISS 2012* (pp. 967-972). Springer Berlin Heidelberg.

Varia, J. (2010). Migrating your Existing Applications to the AWS Cloud. A Phase-driven Approach to Cloud Migration, October 2010. Retrieved from http://docs.huihoo.com/amazon/aws/whitepapers/Migrating-your-Existing-Applications-to-the-AWS-Cloud-October-2010.pdf

Vohradsky, V. (2012). Cloud Risk – 10 Principles and a Framework for Assessment. Retrieved from http://www.isaca.org/Journal/archives/2012/Volume-5/Pages/Cloud-Risk-10-Principles-and-a-Framework-for-Assessment.aspx Accessed 7 November 2016

Ward, C., Aravamudan, N., Bhattacharya, K., Cheng, K., Filepp, R., Kearney, R., Peterson, B., Shwartz, L., & Young, C. (2010). Workload migration into clouds challenges, experiences, opportunities. In *Cloud Computing (CLOUD), 2010 IEEE 3rd International Conference on* (pp. 164-171) July. IEEE.

Whaiduzzaman, M., Gani, A., Anuar, N. B., Shiraz, M., Haque, M. N., & Haque, I. T. (2014). Cloud Service Selection Using Multi-criteria Decision Analysis. *The Scientific World Journal,* Article ID 459375, 10 pages. http://dx.doi.org/10.1155/2014/459375 Computer Society

Zardari, S., & Bahsoon, R. (2011). Cloud adoption: a goal-oriented requirement engineering approach. In *Proceedings of the 2nd International Workshop on Software Engineering for Cloud Computing* (pp. 29-35) May. ACM.

Zhang, Q., Cheng, L., & Boutaba, R. (2010). Cloud Computing: State-of-the-art and Research Challenges. *Journal of Internet Services and Applications, 1*(1), 7–18.

Zhao, J.F., Zhou, J.T. (2014). Strategies and Methods for Cloud Migration. *International Journal of Automation and Computing, 11*(2), 143–152.

Zhu, K. X., & Zhou, Z. Z. (2012). Research note—Lock-in strategy in software competition: Open-source software vs. proprietary software. *Information Systems Research*, *23*(2), 536-545.

Copyrights