CloudComputing and Security

Abílio Cardoso[1] and Paulo Simões[2]
[1]Portucalense University, Portugal
[2]CISUC-DEI, University of Coimbra, Portugal
abilioc@upt.pt
psimoes@dei.uc.pt

Abstract: There is always a strong pressure on Information Technology (IT) to do more with fewer resources. Over the decades, this pressure to rationalize IT costs spurred a number of paradigms, technologies and buzzwords. Some of them failed to meet their promises, while others became successfully embed in IT practices and infrastructures, providing sizeable benefits. The paradigm of cloud computing is currently riding this wave, promising to be the next great revolution in IT. Cloud computing appears to have the right technological and market ingredients to become widely successful. However, there are some key areas where cloud computing is still underperforming – such as security. Availability, security, privacy and integrity of information are some of the biggest concerns in the process of designing, implementing and running IT services based on cloud computing, due to technological and legal matters. There is already an extensive set of recommendations for IT management and IT governance in general – such as the popular Information Technology Infrastructure Library (ITIL) guidelines and Control Objectives for Information and related Technology (COBIT) recommendations. However, the field of cloud computing remains poorly covered. ITIL and other general sources can be sometimes translated to the context of cloud computing, but there are many new challenges not addressed by those generic resources. Recognizing this state of affairs, a number of initiatives already started focusing on novel proposals specifically targeting cloud computing but, up to now, with no significant outcomes. In this paper, we discuss the security implications involved in the migration of IT services to the cloud-computing model, proposing a set of rules and guidelines to be followed in the process of migrating IT services to the cloud. This set of rules and guidelines largely builds on general ITIL recommendations, discussing how to extend/adapt them to the field of cloud computing and identifying which a number of novel areas not covered by current ITIL recommendations.

Keywords: cloud computing, security, ITIL

1. Introduction

The term “cloud computing” was coined in the fourth quarter of 2007, in the context of a joint project between IBM and Google [Vouk, 2008, Zhang et al., 2010b]. However, as also happens with many other emerging trends – and despite being a subject on which much has been written – there is no consensual definition of what cloud computing really means. As an example, in [Vaqueroet al., 2009] there is a list of at least 22 distinct definitions of cloud computing proposed during 2008.

One definition recognized by several authors [Grobauer et al., 2010, Khajeh-Hosseini et al., 2010, Shimba, 2010, Foster et al., 2008, Zhang et al., 2010a] is presented by the National Institute of Standards and Technology (NIST). NIST, adopting a broad scope, defines cloud computing as “a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.” [Mell and Grance, 2011].

Cloud computing is classified in four deployment models: public, private, hybrid and community. In the public model, the cloud resources such as applications, storage and computing, are owned by an organization external to the customer. Customers consume these resources over the Internet in general, either in a free or on a pay-by-use model. Furthermore, the customers share components and resources with others that are unknown to them in a multi-tenant environment. In addition, the customer data might be distributed by various regions around the globe.

In this model, the emphasis is on offering services targeting a wider client base while on the private cloud the focus is having more attention on customization and personalisation of cloud functionalities. Additionally, the service agreements are typically non-negotiable being the service terms entirely established by the cloud-computing service provider, despite there may be some negotiated service agreements. Thus and being the public model an overarching scenario in the cloud computing deployment models this paper the focus is on this model.

Traditionally, each of the aforementioned deployment models is divided into three layers (also known as service models), according to the services it provides to the users. These three layers include, on the first level, Infrastructure-as-a-Service (IaaS), where the user can afford, upon request, processor resources, storage and networking, among others. At this level, the user is required to have specialized technical knowledge and the provider delivers computing power/resources. On a second level, the Platform-as-a-Service (PaaS) layer allows users to implement their applications in the cloud, by using the programming languages and tools provided by the service provider. The third corresponds to Software-as-a-Service (SaaS), where the applications provided by the service provider run in the cloud infrastructure and are typically accessed using a Web browser.

With the large amount of resources it provides for developing and deploying applications and services, the cloud-computing paradigm is an attractive tool to upgrade, extend or replace many of the services hosted by the traditional data centre. Nonetheless, in order to completely fulfil its promises, cloud computing still needs to win the trust of involved stakeholders. A recent survey, which included more than 500 executives and IT managers from 17 countries, revealed that despite the benefits of cloud computing, there is more confidence in internal systems, due to safety threats and loss of control over valuable information. Another survey, from IDC [Gens, 2008], indicates that 74.6% of respondents point safety as the first challenge of cloud computing.

In the traditional data centre there is already an implicit need to trust hardware and software suppliers (as well as in outsourced and own staff), since each of the various components of the system (hardware, software, humans) may potentially compromise the security of information. Nevertheless, it is still possible to improve the protection of information by overlaying additional security schemes in order to obtain a more protected environment – even when there is less confidence in each supplier. A good example of this approach would be the installation of multiple firewalls and intrusion detection systems from different vendors (serially laid out).

However, in cloud computing the custody of information is handed over to a third party. Thus, there is a fundamental difference: while previously in traditional paradigms the information systems can be protected from one specific supplier, in cloud computing all these systems are typically managed by the service provider – resulting in the rather uncomfortable need of completely relying on the cloud service provider.

Whenever an organization analyses the possible migration of its IT services to the paradigm of cloud computing, availability, security, privacy and data integrity are on the top of considerations. These concerns relate with both technological and legal matters, bearing in mind that the service provider can be legally responsible for any security breach in a cloud-based service, but, nonetheless, the client is usually the most severely affected. Therefore, before moving any service to the cloud it is vital to properly understand and model the division of responsibilities, risks and potential impact between the client institution and the cloud service provider. Additionally, the customers must recognize that, despite shifting their IT infrastructure to the cloud they are still responsible for compliance, risk and security management. Otherwise, the expect benefits provided by cloud computing can be counterweighted by the involved risks.

Considering the general field of IT, the Information Technology Infrastructure Library (ITIL) [ITIL,], stands out as a widely recognized reference guideline for IT service management. Published by the Central Communications and Telecommunications Agency (CCTA) and, more recently, the Office of Government Commerce (OGC), ITIL provides a practical, no-nonsense framework for identifying, planning, delivering and supporting IT services to the business. Consisting of a set of good practices, described over five volumes known as Service Strategy, Service Design, Service Transition, Service Operation and Continual Service Improvement, ITIL is currently in Version 3 (known as ITILv3 and ITIL 2011 edition). Promoted by the English government for use in IT companies in 2007, and last updated in 2011, ITILv3 it has been rapidly adopted throughout Europe as the de facto standard for best practices in IT service delivery.

However, the field of cloud computing imposes novel challenges which are not properly covered by ITIL or similar initiatives, such as the Control Objectives for Information and related Technology (COBIT) recommendations. Even though such general sources can be partially translated to the context of cloud computing, there are several areas where the paradigm shift precludes straightforward application. Therefore, it is time to re-think how to handle the process of migrating IT services to the cloud, in order to develop a proper set of guidelines, recommendations and good practices. This paper contributes to such discussion, focusing in the specific area of security, analysing how to extend/adapt ITIL recommendations to the field of cloud computing.

The remaining sections of this paper are organized as follows. Section 2 compares the security challenges imposed by traditional IT services with the problems imposed by the concept of cloud computing. Section 3 discusses the migration of IT services to cloud computing, from the point of view of security. Section 4 discusses how the ITIL best practices could assist in the execution of such migration tasks. Finally, Section 5 concludes the paper.

2. The security challenges introduced by cloud computing

As already mentioned,security, privacy and integrity are some of the biggest concerns in the implementation and use of the cloud computing services [Armbrust et al., 2009]. However,d ata encryption, compliance with standards and service level agreements can be used to minimize security concerns.

From a technical point of view, the majority of security risks associated with cloud computing are already present in traditional data centres (or as argued by [Jansen, 2011] known problems cast in a new setting). Possibly, apart from very specific risks induced by server virtualization (which also exist, to some extent, in traditional data centres using server consolidation), most of the security risks are shared by both paradigms – for instance SQL injection, cross-site scripting, zero-day exploits of applications and operating systems, etc.

Virtualization does increase the impact of some of these risks, since successful attacks on the hosting machine (where the hypervisor is located) may potentially compromise every hosted virtual machine. However, such events can be reasonably avoided and/or controlled using appropriate protection mechanisms for the hosting machines. Faults on the virtualization platforms themselves are also an obvious risk, but up to now, there are very few examples of such faults (and even fewer of negative consequences of such faults).

In simple terms, availability means that an organization has its full set of computing resources accessible and usable at all times [Jansen, 2011]. Availability is also a major concern, even though there are no fundamental differences, from a strictly technical point of view, between traditional services and cloud-based services – except for the possible addition of more network links to the core of critical system components.

The majority of problems, therefore, are not inherently technical. They relate with the implicit need to trust external parties to maintain critical information and provide critical IT services. This need was already present in traditional IT services – whenever new equipment or new applications were deployed in the data centre, there was an implicit need to trust the associated providers. Nonetheless, there is a fundamental difference: in cloud computing it is much more difficult to manage the chain of trust, since there is no clear view – for the client institution – on the way the service is provided. The client only knows the service provider, and the whole web of subcontracted service components is usually opaque or, at most, not verifiable by third parties.

Under the cloud-computing paradigm, an organization relinquishes direct control over many aspects of security and, in doing so, confers an unprecedented level of trust onto the service provider [Jansen, 2011].

In order to maintain its systems protected, the customer needs to gather detailed information about the security-oriented requirements of its IT services, applications and data. This knowledge will be useful when migrating to cloud computing paradigms, since it allows comparing and evaluating traditional services with their cloud-based counterparts.

Before the customer can solve/mitigate the issues on security, he needs to perform a risk assessment to properly identify and evaluate the assets, threats and the possible countermeasures to implement.

Identify and evaluate assets

In traditional data centres, the customer assets encompass information, applications, hardware, network, installations and IT workers. However, the cloud-computing paradigm moves some of the responsibilities from the customer to the cloud provider. For instance, the cloud provider becomes responsible for hardware (in the case of IaaS) or applications and hardware (in the case of SaaS). Therefore, the customer should determine in advance, for the assets to move to the cloud, how valuable they are and what happens if, for instance, information becomes stolen or simply inaccessible.

Identify the threats

After proper identification and evaluation of the assets, it is important to recognise the threats that these assets may suffer. On cloud computing scenarios, security threats may arise from various sources, such as loss of availability, security flows on the cloud provider, other customers of the same cloud provider, attacks from external parties, etc. It is necessary to identify the threats that applications, data and virtual machines may suffer in the cloud.

Identify and apply countermeasures

After identifying the threats, the customer should apply the necessary measures to solve the problems encountered.

3. Security issues in the migration to the cloud

Cloud computing is the latest trend to partially or completely outsource IT operations to run a business from the public cloud that provides a flexible and highly scalable technology platform for an organization's business operations [Dhar, 2011]. The concerns faced by IT managers, when moving servers, applications and data to the cloud computing paradigm, can be grouped in two major sets: the so called *on-premise* and *off-premise*. The first includes all the issues that the IT managers must solve on their own, while the second encompasses the issues that IT managers must answer with the support of the cloud providers.

The *on-premise* set includes issues related with the complete identification of the IT customer solution. This group also encompasses, for instance, the complete and detailed list of all applications, the iteration among them, the identification of the data they use, the related security requirements, special hardware or software requirements, etc.

Data used by the applications also deserves the attention of the IT manager that needs to obtain a detailed definition of information that includes adopted security policies – namely in terms of availability, confidentiality, integrity, availability, access definition and redundancy.

Another important aspect is the infrastructure of network communications, namely external connections. This is a vital issue, since the access to the cloud computing services (and therefore the availability) depend on this communication line. The IT manager should identify the requirements and the costs of these connections, their security and the necessity of backup solutions.

The *off-premise* set encompasses the identification of the relevant providers that best answer to the necessities that were previously defined, as well as the identification of the services offered by each provider– in order to choose the more appropriate for the institution.

The identification of services includes those that are available in each of the service models (IaaS, PaaS and SaaS) and the characteristics of each service, namely the time needed to provision a service, to update, to expand and contract the resources and the service uptime. The organisation must validate what cloud model or models best address its concerns.

The cloud applications are grouped into three major groups, the applications migrated by customer, the applications made available by the cloud provider and the applications used by the provider to manage the cloud.

The applications migrated by the customer to the cloud are made available via IaaS or PaaS models. The customer should inquire the provider to obtain information regarding the degree of security and integrity provided to the applications. Additionally, information should be gathered regarding the backup copies in order to recognize its periodicity, location, validity and the possibility of make backup copies of data from the cloud among others. Moreover it is needed to identify what are the import and export facilities provided, specifically in terms of portability with the applications from other providers, what are the associated costs and what are the standards used to transfer the applications to and from another provider and from the customer institution to the cloud.

The applications made available by the service provider, typically via SaaS model, also need the attention of the team in charge of the move to cloud. The customer needs to recognize what customizations of applications are suitable to the institution needs, which the security measures are needed to assure the requirements, the details on how the information backup is processed, and by whom those applications are developed and tested.

The group of applications that the cloud provider uses to manage its services also need similar care from the costumer.

The data is another important issue in the cloud-computing paradigm requiring that the customer request information on where the information stored, since different locations may have different jurisdictions. Additionally, the customer needs to know who manage the storage, the cloud provider or a third party and what the costs are. The data security also needs special attention. Therefore it is need to know who have access to data, systems administrators, network managers or other employees, how often are the backup copies made and what types and levels of encryption that the provider can offer in order to ensure that data cannot be read notwithstanding was stolen.

As said, the security is on top of the top of concerns when moving services and data to cloud computing. Thus, the customer and the cloud provider must clearly identify what are their responsibilities and the responsibilities of other stakeholders in the process like staff responsible for the management of systems, including systems administrators, network managers and other employees. Additionally the customer needs to gather information concerning the provider employees such as training certifications and background.

To validate that the provider meets the applications security requirements previously identified, the customer need to request additional information form the provider regarding access management, namely the authentication mechanisms available and the level of integration that can be done with in-house authentication. The security issues should also encompass the cloud provider infrastructure that is, equipment, network, security standards and the provider security certifications. Knowing the security certifications of the various providers could assist the customer on the selection of the service provider.

The recording of the actions, the errors and the results (logs) by the service provider is an additional security issue that the customer should be concerned. Besides gathering the details of the information registered, the customer must also know how long the records are kept, identify who has access to them, in what way and as said by[Marston et al., 2011] confirm how long the information is stored to allow, if necessary, forensic analysis .

The Service Level Agreement defines a written agreement, negotiated between the customer and the service provider, which documents the agreed service levels and the respective costs. The SLA should include, in terms of security, service uptime, problem solution time, performance, response time, security measures, terms definition.[Cochran and Witman, 2011] emphasizes the importance of records and SLA when they state that the SLA should clearly identify the data that administrators have access and whether or not there are records of personal data. A more detailed discussion about the SLA can be found in [Kandukuri et al., 2009].

Another author [Patel et al., 2009] also highlight the SLA prominence in the cloud computing paradigm stating " As more costumers delegate their tasks to cloud computing service providers, the service level agreements between customers and service providers emerge as a key aspect".

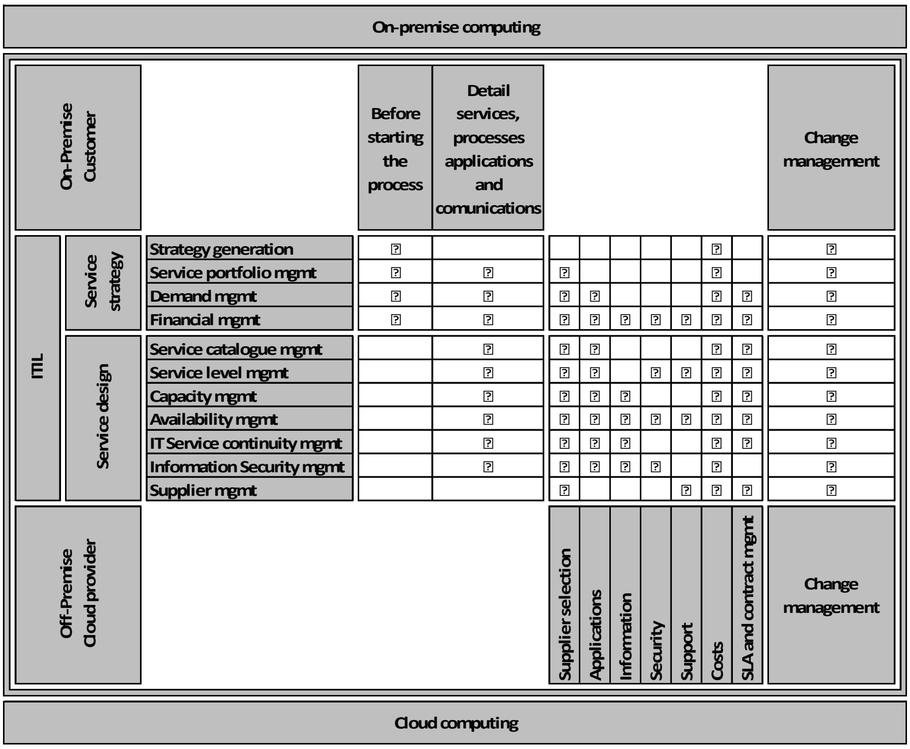
In short, the SLA forms an integral part of a client's first line of defence [Ramgovind et al., 2010].

4. ITIL and the security when moving to cloud

The migration to the cloud-computing paradigm is a complex task that needs the right tools to be more easily, with more control and in a more accurate way accomplished. Whereas in section 3 were presented the various activities and issues that must be engaged by the institution, with and without the cloud providers cooperation, in this section is presented, from the point of view of security, how ITIL could be the right tool to assist on the move to cloud computing.

The security issues presented are similar to the tasks and problems found in the management of the traditional IT services life cycle. Therefore and being the ITIL framework a set of good practices for the identification, planning, delivering and supporting of IT services, could be used to solve the security issues presented and support the institution in the development of those activities. Additionally ITIL facilitate communication between service providers and customers [Nehme et al., 2009], the two main actors in the migration to the cloud computing. Although it was published in July 2011 an update to the current version, 3 of ITIL (ITIL 2011 edition) did not seem necessary to recast the work as it still is not to our knowledge that has already been implemented in an institution.

Figure 1presents the relationship between the processes defined in the first two ITIL books and the activities and issues presented in order to obtain a broader perspective of the interaction between ITIL and the migration to the cloud computing. However, in the in the following paragraphs, are shown those that have a close relationship with security.



On-premise computing

On-Premise Customer

ITIL			Before starting the process	Detail services, processes applications and comunications	Supplier selection	Applications	Information	Security	Support	Costs	SLA and contract mgmt	Change management
ITIL	Service strategy	Strategy generation	⍰							⍰		⍰
		Service portfolio mgmt	⍰	⍰	⍰					⍰		⍰
		Demand mgmt	⍰	⍰	⍰	⍰				⍰	⍰	⍰
		Financial mgmt	⍰	⍰	⍰	⍰	⍰	⍰	⍰	⍰	⍰	⍰
	Service design	Service catalogue mgmt		⍰	⍰	⍰				⍰	⍰	⍰
		Service level mgmt		⍰	⍰	⍰		⍰	⍰	⍰	⍰	⍰
		Capacity mgmt		⍰	⍰	⍰	⍰			⍰	⍰	⍰
		Availability mgmt		⍰	⍰	⍰	⍰	⍰	⍰	⍰	⍰	⍰
		IT Service continuity mgmt		⍰	⍰	⍰	⍰			⍰	⍰	⍰
		Information Security mgmt		⍰	⍰	⍰	⍰	⍰		⍰		⍰
		Supplier mgmt			⍰				⍰	⍰	⍰	⍰

Off-Premise Cloud provider

Cloud computing

Figure 1: ITIL and the move to cloud computing

Service Catalogue Management

According to [Taylor, 2007] the objective of the service catalogue management is to manage the information contained within the service catalogue and to ensure that it is accurate and reflects the current details, status, interfaces and dependencies of all services that are being run or being prepared to run in the live environment. An accurate and consistent picture of the services made available by the institution is crucial to know what services could be moved to the cloud, what resources and security are needed by those services.

Service Level Management

The Service Level Management objectives embrace the monitoring and the improving of customer satisfaction with the quality of services delivered. The achievement of these objectives supportsthe cloud computing migration and maintenance. While monitoring the SLA the customer also certifies the quality of services provided by the cloud provider ensuring that the cloud services are provided in accordance with the contract. The security issues found in other ITIL process must be reflected in the SLA in order to have a written agreement with the provider in order to ensure that the customer's security needs are met.

Information Security Management

As stated in the previous sections the security is one of the major concerns with when adopting the cloud-computing paradigm. Therefore, the Information Security Management (ISM) is a key concern area being mandatory to ensure the integration between IT security and business security. The purpose of the ISM process is [Lloyd et al., 2007] to ensure that the security aspects with regard to services and all Service Management activities are appropriately managed and controlled in line with business needs and risks.

The Information security management could assist the migration to cloud computing in the same way it interacts with service level management, that is, support in determining of security requirements and responsibilities and their inclusion within Service Level Reports (SLRs) and SLAs.

The move to the cloud-computing paradigm entails a shift of some of security responsibilities from the customer to the service provider. However, the ultimate accountability, in terms of information security, always rests with the customer itself.

Availability Management

The goal of the Availability Management is to ensure that the level of service availability delivered in all services is matched to or exceeds the current and future agreed needs of the business, in a cost-effective manner [Lloyd et al., 2007]. Despite the ITIL Availability Management be a very important process in the migration to the cloud-computing paradigm, afterwards the services are migrated to the cloud it is difficult for the customer, to obtain the same information that it has in-house from service provider to maintain same level in the availability management. However, much of the responsibility of availability management is transferred to the cloud computing service provider.

5. Conclusion

Cloud computing encompasses various technologies, such as computing networks, virtualization, operating systems, used in the traditional data centres leading to that it may suffer some security problems associated with such technologies. While in the IT departments and datacentres the manager may install multiple firewalls and intrusion detection systems from different vendors (serially laid out) in order to protect the information in the cloud computing environment the customer must trust in the providers the security of his information and applications.

The migration to cloud computing has various security challenges. The use of the ITIL methodology either to obtain the necessary information either to point the appropriate methodology are an important assistance for the resolution of such issues.

The share of responsibilities between the customer and the cloud service provider governed by ITIL presented, as an approach to solving the security issues in the moving to cloud computing, has several advantages. The use of ITIL by both the customer and the provider facilitates their communication, making clear the interaction between them - since they speak the same language. Additionally this shared responsibility also comes from the point of view that each one has about security. The security is important, for the customer, to protect its data and applications and, in some cases, as a measure for the continuation of its business. For the service provider is a way to safeguard the assets entrusted to it and form the basis of the business. Moreover, security and trust between customer and supplier are crucial to the provider selection.

References

Armbrust et al., 2009 Armbrust, M., Fox, A., Griffith, R., Joseph, A. D., Katz, R. H., Konwinski, A., Lee, G., Patterson, D. A., Rabkin, A., Stoica, I., and Zaharia, M. (2009). Above the clouds: A berkeley view of cloud computing. Technical Report UCB/EECS-2009-28, EECS Department, University of California, Berkeley.

Cochran and Witman, 2011Cochran, M. and Witman, P. (2011). Governance and service level agreement issues in a cloud computing environment. *Journal of Information Technology Management*, 22(2):41.

Dhar, 2011 Dhar, S. (2011). From outsourcing to cloud computing: Evolution of it services. In *Technology Management Conference (ITMC), 2011 IEEE International*, pages 434 –438.

Foster et al., 2008 Foster, I., Zhao, Y., Raicu, I., and Lu, S. (2008). Cloud computing and grid computing 360-degree compared. In *2008 Grid Computing Environments Workshop*, pages 1–10. IEEE.

Gens, 2008 Gens, F. (2008). It cloud services user survey, pt.2: Top benefits & challenges. Available online at http://blogs.idc.com/ie/?p=210.Seen in: 2010.09.11.

Grobauer et al., 2010 Grobauer, B., Walloschek, T., and Stocker, E. (2010).Understanding cloud-computing vulnerabilities.*Security Privacy, IEEE*, PP(99):1–1.

ITIL, ITIL.Information Technology Infrastructure Library (ITIL).A>vailable online at http://www.itil-officialsite.com.Seen in: 2010.04.17.

Jansen, 2011Jansen, W. (2011). Cloud hooks: Security and privacy issues in cloud computing. In *System Sciences (HICSS), 2011 44th Hawaii International Conference on*, pages 1 –10.

Kandukuri et al., 2009 Kandukuri, B., Paturi, V., and Rakshit, A. (2009).Cloud security issues.In *Services Computing, 2009.SCC '09.IEEE International Conference on*, pages 517 –520.

Khajeh-Hosseini et al., 2010 Khajeh-Hosseini, A., Greenwood, D., Smith, J. W., and Sommerville, I. (2010). The Cloud Adoption Toolkit: Addressing the Challenges of Cloud Adoptionin Enterprise.*CoRR*, abs/1003.3866:1–10.

Lloyd et al., 2007 Lloyd, V., Rudd, C., and Taylor, S. (2007). *OCG Books ITIL - Service Design*. TSO (The Stationery Office).

Marston et al., 2011 Marston, S., Li, Z., Bandyopadhyay, S., and Ghalsasi, A. (2011). Cloud computing - the business perspective. In *System Sciences (HICSS), 2011 44th Hawaii International Conference on*, pages 1 –11.

Mell and Grance, 2011 Mell, P. and Grance, T. (2011).Cloud computing.Available online at http://csrc.nist.gov/-publications/nistpubs/800-145/SP800-145.pdf.Published date: September 2011.Seen in: 2011.10.22.

Nehme et al., 2009 Nehme, J., Persson, M., and Lahiji, S. (2009).*How can ITIL influence IT outsourcing*©.PhD thesis, JÖNKÖPING INTERNATIONAL BUSINESS SCHOOL.

Patel et al., 2009] Patel, P., Ranabahu, A., and Sheth, A. (2009). Service Level Agreement in Cloud Computing. *Cloud Workshops at OOPSLA09*, 1:1–10.

Ramgovind et al., 2010 Ramgovind, S., Eloff, M., and Smith, E. (2010). The management of security in cloud computing. In *Information Security for South Africa (ISSA), 2010*, pages 1 –7.

Shimba, 2010 Shimba, F. (2010).*Cloud Computing: Strategies for Cloud Computing Adoption*. PhD thesis, Dublin Institute of Technology,.

Taylor, 2007 Taylor, S., editor (2007).*ITIL – The Official Introduction to the ITIL Service Lifecycle*.TSO, London.

Vaqueroet al., 2009 Vaquero, L. M., Rodero-Merino, L., Caceres, J., andLindner, M. (2009). A break in the clouds: towards a cloud definition.*SIGCOMM Comput.Commun. Rev.*, 39(1):50–55.

Vouk, 2008 Vouk, M. (2008).Cloud computing: Issues, research and implementations.In *Information Technology Interfaces, 2008.ITI 2008.30th International Conference on*, pages 31–40.

Zhang et al., 2010a Zhang, Q., Cheng, L., and Boutaba, R. (2010a). Cloud computing: state-of-the-art and research challenges.*Journal of Internet Services and Applications*, 1:7–18. 10.1007/s13174-010-0007-6.

Zhang et al., 2010b Zhang, S., Zhang, S., Chen, X., and Huo, X. (2010b). Cloud computing research and development trend. *Future Networks, 2010. ICFN "10. Second International Conference on*, 0:93–97.